ceis

ETUDE PROSPECTIVE ET STRATEGIQUE

Analyse du *Manuel de Tallinn 2.0* *sur le droit international applicable aux cyber-opérations*

Novembre 2017

Marché n° 2015 1050 129 916 – BC n° 1403840502

Étude financée par le ministère des Armées

DGRIS
Direction générale des relations internationales et de la stratégie
MINISTÈRE DES ARMÉES

Le ministère des Armées fait régulièrement appel à des prestataires extérieurs pour réaliser des études, selon une approche géographique ou sectorielle, visant à compléter son expertise interne. Ces relations contractuelles s'inscrivent dans le développement de la démarche prospective de défense qui, comme le souligne le dernier Livre blanc sur la défense et la sécurité nationale, « *doit pouvoir s'appuyer sur une réflexion stratégique indépendante, pluridisciplinaire, originale, intégrant la recherche universitaire comme celle des instituts spécialisés* ».

Une grande partie de ces études sont rendues publiques et mises à disposition sur le site du ministère des Armées. Dans le cas d'une étude publiée de manière parcellaire, la Direction générale des relations internationales et de la stratégie peut être contactée pour plus d'informations.

AVERTISSEMENT : Les propos énoncés dans les études et observatoires ne sauraient engager la responsabilité de la Direction générale des relations internationales et de la stratégie ou de l'organisme pilote de l'étude, pas plus qu'ils ne reflètent une prise de position officielle ou officieuse du ministère des Armées.

Analyse du *Manuel de Tallinn 2.0 sur le droit international applicable aux cyber opérations*

Étude réalisée par François Delerue

Étude prospective et stratégique (EPS) – bon de commande CC–2016–17

Version finale – mercredi 29 novembre 2017

Tables des matières

Note liminaire

Cette étude prospective et stratégique (EPS) a été réalisée par François Delerue pour le compte du ministère des Armées (bon de commande CC-2016-17).

L'auteur tient à remercier les différentes personnes l'ayant soutenu et aidé dans la réalisation de cette étude. Il tient particulièrement à remercier Aude Géry pour ses précieux conseils et commentaires sur les différentes versions de cette étude.

Il a réalisé cette étude en sa capacité personnelle, par conséquent les idées exprimées, mais aussi les éventuelles erreurs présentes dans cette étude n'engagent que l'auteur en sa capacité personnelle et ne peuvent être associées ou attribuées à aucune autre personne ou institution.

1 Introduction

Cette analyse a une double vocation. Premièrement, offrir un résumé des règles du *Manuel de Tallinn 2.0 sur le droit applicable aux cyber opérations* en français, permettant ainsi au lecteur francophone de disposer d'un document relativement court retraçant le contenu des règles du *Manuel de Tallinn 2.0*. Deuxièmement, offrir une analyse des points clefs du *Manuel de Tallinn 2.0*, notamment des points les plus sensibles et ceux où l'approche du *Manuel* pourrait être considérée comme discutable.

L'analyse et le commentaire des règles du *Manuel de Tallinn 2.0* sont précédés d'une brève introduction permettant au lecteur de se familiariser avec le cadre dans lequel le *Manuel* a été réalisé et de comprendre l'impact de ce document au regard de la pratique du droit international. Par ailleurs, cette introduction met en perspective les deux éditions du *Manuel de Tallinn*.

1.1 Le Centre d'excellence de cyberdéfense coopérative de l'OTAN (NATO CCD COE)

Le Centre d'excellence de cyberdéfense coopérative de l'OTAN (NATO CCD COE) a été créé à Tallinn en Estonie par la signature le 14 mai 2008 d'un protocole d'accord entre l'Allemagne, l'Espagne, l'Estonie, l'Italie, la Lettonie, la Lituanie et la Slovaquie. Il s'agit d'une organisation indépendante qui dispose donc de son budget et de personnel propres et est composée d'États membres. Le NATO CCD COE est devenu une organisation internationale militaire liée à l'OTAN en octobre 2008[1] par décision du Conseil de l'Atlantique nord[2].

Tous les États membres de l'OTAN peuvent devenir membres du NATO CCD COE. En 2017, 16 États membres de l'OTAN (Allemagne, Espagne, Estonie, États-Unis, France, Grèce, Hongrie, Italie, Lettonie, Lituanie, Pays-Bas, Pologne, République tchèque, Royaume-Uni, Slovaquie et Turquie) ont déjà rejoint le Centre d'excellence comme « *Sponsoring Nations* ». S'ajoutent également deux États non membres de l'OTAN (Autriche et Finlande) qui participent comme « *Contributing Participants* » et qui devraient bientôt être rejoints par la Suède.

La mission du Centre d'excellence est d'améliorer les capacités, la coopération et le partage d'information entre l'OTAN, les États membres et les États partenaires de l'OTAN dans le domaine de la cyberdéfense par le biais d'actions de formation, de recherche et développement, de partage d'expériences et de consultations.

1.2 Le *Tallinn Manual Process*

En 2009, le NATO CCD COE a demandé à un groupe d'experts internationaux de préparer un manuel sur le droit international applicable à la cyberguerre. Ce groupe d'experts internationaux était dirigé par le Professeur Michael N. Schmitt[3] et regroupait 23 experts d'origines et de professions diverses[4]. Aucun français n'a pris part à ce groupe. Ces experts intervenaient en leur nom propre et leurs travaux, bien que financés par le Centre d'excellence, n'ont pas vocation à devenir la doctrine juridique officielle du NATO CCD COE, de l'OTAN ou de leurs États membres ou partenaires.

---

1 http://www.nato.int/cps/en/natohq/official_texts_17300.htm

2 https://ccdcoe.org/centre-first-international-military-organization-hosted-estonia.html

3 Voir la biographie du Professeur Michael N. Schmitt sur le site de l'Université d'Exeter : https://socialsciences.exeter.ac.uk/law/staff/mschmitt/

4 SCHMITT M.N. et L. VIHUL (dir.), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2e éd., Cambridge University Press, 2017, p. xix-xx.

Les travaux de ce groupe d'experts internationaux ont débouché sur la publication en 2013 chez Cambridge University Press du *Manuel de Tallinn sur le droit international applicable à la cyberguerre*[5] (*Manuel de Tallinn 1.0*). Cette première édition du *Manuel de Tallinn* se concentrait sur le droit applicable aux cyber opérations les plus graves, à savoir celles qui constituaient un recours à la force, une agression armée ou qui prenaient part à un conflit armé. Par conséquent, le *Manuel de Tallinn 1.0* analysait principalement le droit international du recours à la force, aussi connu sur le nom de *jus ad bellum* ou de *jus contra bellum*, et le droit des conflits armés, aussi connu sous le nom de *jus in bello*. Ce choix explique aussi l'utilisation du terme « cyberguerre » dans le titre de l'ouvrage.

Ce choix a été fortement critiqué en ce que la vaste majorité des cyber opérations demeurent sous le seuil du recours à la force et n'ont pas lieu dans le cadre d'un conflit armé et que, par voie de conséquence, ni le *jus contra bellum* ni le *jus in bello* ne leur sont applicables.

Dès 2013, il a été décidé de convier un nouveau groupe d'experts internationaux, toujours sous la direction du Professeur Michael N. Schmitt, pour étudier le droit international applicable aux cyber opérations en temps de paix. Les travaux des 21 experts[6] prenant part à ce nouveau groupe ont débouché sur la publication en 2017 de la seconde édition du *Manuel de Tallinn*, le *Manuel de Tallinn 2.0 sur le droit international applicable aux cyber opérations* (*Manuel de Tallinn 2.0*). Le premier groupe d'experts avait été critiqué quant à l'origine géographique de ses membres, pour beaucoup issues du monde anglo-saxon. Le second groupe avait une meilleure diversité géographique avec notamment la présence de membres asiatiques[7]. À nouveau, il convient de souligner qu'aucun français n'a pris part à ce groupe d'experts.

1.3 Autorité et influence du *Manuel de Tallinn*

Il convient de souligner que les deux éditions du *Manuel de Tallinn* ne sont pas des documents officiels ou l'expression de la position du NATO CCD COE, de l'OTAN ou de leurs États membres ou partenaires[8]. Ces documents sont, en effet, le fruit du travail d'experts indépendants intervenant en leur capacité personnelle.

Force est de constater, néanmoins, que la première édition du *Manuel de Tallinn* a eu une influence très grande sur la perception des États, des professionnels et des universitaires, du droit international applicable aux cyber opérations. Différentes raisons permettent d'expliquer cette situation.

Tout d'abord, les experts ayant participé à la préparation des deux éditions du *Manuel de Tallinn* sont parmi les plus grands spécialistes du domaine. Ainsi, les membres universitaires de ces groupes ont contribué au *Manuel de Tallinn* avec leurs travaux, mais ont aussi utilisé le *Manuel de Tallinn* dans leurs travaux et leurs enseignements.

Deuxièmement, la réputation des experts a également fortement contribué à assoir la notoriété du *Manuel de Tallinn*.

Troisièmement, le *Manuel de Tallinn* offre une des rares études approfondies du droit international existant, et se distingue des autres études par son approche résolument pratique, ce qui en fait un document incontournable. En effet, à l'inverse d'un travail purement académique ayant vocation

---

5 SCHMITT M.N. (dir.), *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013.

6 SCHMITT M.N. et L. VIHUL (dir.), *The Tallinn Manual 2.0*, *op. cit.*, p. xii-xiii.

7 LIU I.Y., « The due diligence doctrine under Tallinn Manual 2.0 », *Computer Law & Security Review: The International Journal of Technology Law and Practice*, juin 2017, vol. 33, n° 3, p. 391.

8 SCHMITT M.N. et L. VIHUL (dir.), *The Tallinn Manual 2.0*, *op. cit.*, p. 2.

à analyser et discuter le droit applicable, le *Manuel de Tallinn* se présente sous forme de règles suivies d'un commentaire le rendant plus opérationnel.

L'impact du *Manuel de Tallinn* dans l'enseignement et la formation ne doit pas être sous-estimé. À titre d'exemple, le séminaire sur le droit international des cyber opérations (*international law of cyber operations seminar*) organisé par le NATO CCD COE est aujourd'hui une des formations principales dans le domaine à laquelle participent un certain nombre de personnes venues des États membres et partenaires de l'OTAN. Le programme de cette formation est articulé, au moins pour partie, autour du *Manuel de Tallinn* et un exemplaire est remis aux participants. Encore une fois, l'organisation interne du *Manuel de Tallinn* en fait un des documents les plus à même de servir de base pour un programme de formation.

Ces différentes raisons font des deux éditions du *Manuel de Tallinn* des sources[9] particulièrement influentes et incontournables sur le droit international applicable aux cyber opérations.

Le travail effectué par les deux groupes d'experts est remarquable et doit être salué pour sa grande clarté, sa qualité et, dans une certaine mesure, son exhaustivité. Il convient néanmoins de souligner que ces documents n'ont pas valeur contraignante, il ne s'agit pas d'un traité ou d'une convention internationale ni même de la doctrine officielle d'une organisation internationale ou d'un État, et qu'ils ne constituent que l'analyse du droit applicable par un groupe d'experts.

Dans cette perspective il convient de garder une approche critique des règles et commentaires contenus dans les deux éditions du *Manuel de Tallinn*. Elles représentent l'interprétation du droit international existant faite par les groupes d'experts[10]. Ces règles et commentaires peuvent différer dans certains cas des approches qu'auraient certains États, organisations internationales ou courants de doctrine universitaire sur les questions juridiques développées. Il existe une littérature fournie sur ce point.

---

9 Aux termes de l'article 38 du Statut de la Cour international de Justice, « la doctrine des publicistes les plus qualifiés des différentes nations » sont considérés comme des « moyen auxiliaire de détermination des règles de droit », c'est-à-dire des sources secondaires du droit international par opposition aux sources primaires que sont les conventions internationales, la coutume internationale et les principes généraux de droit reconnus par les nations civilisées.

10 Rebecca Ingber, dans un article préparé dans le cadre du *Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* revient sur la démarche et l'influence du *Manuel de Tallinn 2.0* au regard de l'interprétation du droit international. INGBER R., « Interpretation Catalysts in Cyberspace [*Symposium:* Tallinn Manual 2.0 *on the International Law Applicable to Cyber Operations*] », *Texas Law Review*, 2017 2016, vol. 95, p. 1531‑1554.

Kubo Mačák dans un article sur la réticence des Etats à adopter des normes de droit international contraignant à propos du cyberespace et des comportements numériques et le rôle des acteurs non-étatiques dans le développement de normes et interprétations non-contraignantes du droit international applicable, analyse brièvement l'influence des deux éditions du *Manuel de Tallinn* dans cette perspective. MAČÁK K., *From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers*, Rochester, NY, Social Science Research Network, 2017.

2 Présentation des deux éditions du *Manuel de Tallinn*

Le *Manuel de Tallinn 2.0 sur le droit international applicable aux cyber opérations* reprend la plupart des règles et commentaires de la première édition auxquels de nouvelles règles et leurs commentaires viennent s'ajouter.

Ainsi, les troisième et quatrième parties du *Manuel de Tallinn 2.0* dédiées à la paix et la sécurité internationales et les cyber activités (Part III. International peace and security and cyber activities – pp. 301 à 371 – règles 65 à 79) et au droit des cyber conflits armés (Part IV. The law of cyber armed conflict – pp. 373 à 562 – règles 80 à 154) reprennent, à partir de la règle 68 sur l'interdiction du recours à la menace ou à l'emploi de la force, les règles du *Manuel de Tallinn 1.0* sur le droit du recours à la force et le droit des conflits armés avec quelques modifications concernant certaines règles et certains commentaires.

Les 67 premières règles du *Manuel de Tallinn 2.0* sont nouvelles, certaines étant basées sur des règles de la première édition qui ont été complètement revues et développées.

La première partie du *Manuel de Tallinn 2.0* s'intéresse à l'application du droit international général au cyberespace (Part I. General international law and cyberspace – pp. 9 à 176 – règles 1 à 33). Cette première partie est probablement la plus importante du *Manuel de Tallinn 2.0* puisqu'elle s'intéresse aux questions de souveraineté, de *due diligence*, de juridiction, et de droit international de la responsabilité des États et des organisations internationales. En ce sens, le quatrième chapitre est le plus fondamental puisqu'il traite du droit de la responsabilité internationale et détaille ainsi les questions de l'attribution des cyber opérations, de leur licéité au regard du droit international général (sans préjudice des autres parties traitant de la licéité au regard du *jus contra bellum* et du *jus in bello*), des obligations résultant du droit de la responsabilité internationale et finalement de la question des contre-mesures.

La deuxième partie est dédiée à certains régimes spécifiques du droit international (Part II. Specialised regimes of international law and cyberspace – pp. 177 à 300 – règles 34 à 64). Les régimes pris en compte sont le droit international des droits de l'homme, le droit diplomatique et consulaire, le droit de la mer, le droit aérien, le droit spatial et le droit des télécommunications internationales.

Les deux dernières parties (*Part III* et *Part IV*), comme indiqué précédemment, reprennent les règles de la première édition du *Manuel de Tallinn* sur le *jus contra bellum* et le *jus in bello*. Les trois premières règles de la troisième partie (règles 65, 66 et 67) sont des nouveaux ajouts portant sur le règlement pacifique des différends et l'interdiction des interventions par les États et l'Organisation des Nations Unies (ONU).

3 Analyse du contenu du *Manuel de Tallinn 2.0* [11]

3.1 Introduction

L'introduction du *Manuel de Tallinn 2.0*, préparée par le Professeur Michael N. Schmitt, directeur du projet, présente le fonctionnement des deux groupes d'experts internationaux ayant rédigé les deux éditions du *Manuel de Tallinn*, la manière dont elles ont été préparées, l'autorité du *Manuel de Tallinn*, l'organisation interne du *Manuel de Tallinn* et la relation entre les règles et les commentaires[12]. Ces différents éléments ont été abordés précédemment dans cette note et ne seront donc pas détaillés ici.

3.2 Droit international général (Part I. General international law and cyberspace – pp. 9 à 176 – règles 1 à 33)

Le *Manuel de Tallinn 2.0* s'ouvre logiquement sur une première partie traitant de l'application du droit international général au cyberespace. Les quatre premiers chapitres détaillent l'application de normes et principes du droit international, et la façon dont ils viennent réglementer la conduite de cyber opérations. Le cinquième et dernier chapitre traite du régime juridique de l'espionnage et des cyber opérations conduites par des acteurs non étatiques et non attribuables à un État.

La première règle traite directement de la question de l'applicabilité du principe de souveraineté dans le cyberspace. Il aurait été souhaitable, à notre avis, d'ajouter une règle liminaire précisant qu'en droit international rien n'interdit aux États de se doter de capacités numériques et de conduire des cyber opérations. En effet, les cyber opérations ne sont pas illicites en elles-mêmes, par contre elles peuvent violer des normes et principes du droit international.

Ce rappel aurait eu l'avantage de fournir au lecteur, avant qu'il ne se lance dans les méandres de l'applicabilité et de l'application du droit international au cyberespace et aux cyber opérations, le régime juridique général des cyber opérations.

Il convient de souligner que la question de la licéité des cyber opérations en général diffère de celle de la liberté des États de mener des cyber opérations dans la conduite de leurs relations internationales traitée dans la règle 3. En effet, d'un côté il s'agit de l'appréciation de la licéité des cyber opérations au regard du droit international général, de l'autre côté, il s'agit de la liberté d'action des États sur le plan international comme corolaire de leur souveraineté. Ce sont deux questions distinctes.

---

11 Eric Talbot Jensen a publié un résumé en anglais des règles du *Manuel de Tallinn 2.0*, mettant en lumière les principaux désaccords entre les experts ayant participé au *Tallinn Manual Process* et analysant quelques points clefs. Il adopte une approche différente de la présente analyse, puisqu'il se concentre sur quelques points clefs du *Manuel de Tallinn 2.0* et ne fait donc pas une approche exhaustive des règles. JENSEN E.T., « The Tallinn Manual 2.0: Highlights and Insights », *BYU Law Research Paper No. 17-10*, 2017.

12 Michael N. Schmitt a publié un article où il revient sur les différents points abordés dans les deux éditions du *Manuel de Tallinn* et qui mériteraient d'être étudiés plus en avant : la souveraineté, le principe de non-intervention, l'obligation de diligence, l'attaque en droit international humanitaire, l'emploi de la force et la légitime défense. SCHMITT M.N., « Grey Zones in the International Law of Cyberspace », *The Yale Journal of International Law Online*, 2017, vol. 42, n° 2, p. 1‑21. Il s'était livré à un exercice similaire après la publication de la première édition du *Manuel de Tallinn*: SCHMITT M.N., « The Law of Cyber Warfare: *Quo Vadis?* », *Stanford Law & Policy Review*, 2014, vol. 25, p. 269.

3.2.1 Souveraineté (Chapitre 1 – règles 1 à 5)

Le premier chapitre traite d'un des piliers du droit international : la souveraineté[13].

3.2.1.1 Souveraineté numérique

Le principe de souveraineté s'applique au cyberespace (**règle 1**). L'applicabilité du principe de souveraineté avait été affirmée par le Groupe d'experts gouvernementaux (GGE) chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale dans les rapports de 2013 et de 2015[14]. Les deux règles suivantes distinguent les éléments externe et interne de la souveraineté de l'État. D'un côté, **l'État exerce sa souveraineté sur les systèmes d'information, les personnes et les cyber activités sur son territoire, dans les limites de ses obligations découlant du droit international** (**règle 2**). D'un autre côté**, l'État est libre de mener des cyber opérations dans la conduite de ses relations internationales, à condition de respecter ses obligations découlant du droit international** (**règle 3**).

---

13 La Société américaine de Droit international a organisé un *Symposium on sovereignty, cyberspace, and Tallinn Manual 2.0* qui a donné lieu à plusieurs publications interessantes sur le sujet :

- Gary P. Corn et Robert Taylor reviennent sur l'application du principe de souveraineté dans le cyberespace et ses conséquences. Il critique l'approche du *Manuel de Tallinn 2.0* car selon eux le principe de souveraineté serait seulement un principe de droit international coutumier mais pas une norme contraignante *per se*. CORN G.P. et R. TAYLOR, « Sovereignty in the Age of Cyber », *AJIL Unbound*, ed 2017, vol. 111, p. 207-212 ; voir aussi: CORN G.P., *Tallinn Manual 2.0 – Advancing the Conversation*, https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/.
- Les deux directeurs de la publication du *Manuel de Tallinn 2.0*, Michael N. Schmitt et Liis Vihul, répondent aux critiques formulées dans l'article précédent et reviennent sur les différentes approches de la transposition de la souveraineté des Etats dans le cyberespace. SCHMITT M.N. et L. VIHUL, « Sovereignty in Cyberspace: *Lex Lata Vel Non*? », *AJIL Unbound*, 2017, vol. 111, p. 213-218. Par ailleurs, dans un article préparé dans le cadre du *Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* ils reviennent sur l'approche du *Manuel de Tallinn 2.0* sur la souveraineté des Etats et sur les différentes autres approches existantes sur cette question. VIHUL L. et M.N. SCHMITT, « Respect for Sovereignty in Cyberspace Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations », *Texas Law Review*, 2017 2016, vol. 95, p. 1639-1670. Voir aussi: SCHMITT M.N., « Grey Zones in the International Law of Cyberspace », *op. cit.*, p. 4-7.
- Phil Spector affirme que la souveraineté est un principe de droit coutumier, reprenant ainsi l'approche adoptée par le *Manuel de Tallinn 2.0* auquel il a contribué : SPECTOR P., « In Defense of Sovereignty, in the Wake of Tallinn 2.0 », *AJIL Unbound*, 2017, vol. 111, p. 219-223.
- Ahmed Ghappour revient sur le droit coutumier de la souveraineté, et plus particulièrement sur les tensions existantes entre les pratiques des forces de l'ordre dans le cyberespace ayant une dimension potentiellement transnationale et le respect de la souveraineté étatique. GHAPPOUR A., « Tallinn, Hacking, and Customary International Law », *AJIL Unbound*, 2017, vol. 111, p. 224-228.
- Voir aussi l'introduction du symposium : GINSBURG T., « Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0 », *AJIL Unbound*, 2017, vol. 111, p. 205-206.

Sur le traitement de la souveraineté dans le *Manuel de Tallinn 2.0*, voir aussi : WOODS A.K., *The Tallinn Manual 2.0, Sovereignty 1.0*, https://www.lawfareblog.com/tallinn-manual-20-sovereignty-10 ; JENSEN E.T., « The Tallinn Manual 2.0 », *op. cit.*, p. 7-10.

14 ASSEMBLEE GENERALE DES NATIONS UNIES, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale*, document des Nations Unies A/68/98, 2013, para 20 ; ASSEMBLEE GENERALE DES NATIONS UNIES, *Rapport du Groupe d'experts gouvernementaux chargé d'examiner les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale*, document des Nations Unies A/70/174, 2015, paras 27 et 28(b).

Le commentaire sous la première règle commence par détailler l'origine et le contenu du principe de souveraineté et sa relation avec d'autres principes et normes du droit international, ce que nous ne ferons pas dans cette note (commentaire sous la règle 2 – §9, p. 13).

De la même manière que le principe de souveraineté s'applique au cyberespace, les limites que le droit international, notamment le droit coutumier, impose à la souveraineté des États s'appliquent aussi aux cyber activités (commentaire sous la règle 1 – §4, p. 12).

Dans le cadre du *Manuel de Tallinn*, les experts considèrent que le principe de souveraineté s'applique aux couches physique, logique et sociale du cyberespace (commentaire sous la règle 1 – §4, p. 12 ; commentaire sous la règle 2 – §§3-88, pp. 13-15). Ainsi, le principe de souveraineté est applicable aussi bien aux infrastructures physiques sur lesquelles repose le cyberespace, notamment les serveurs, les ordinateurs et les câbles (couche physique), qu'aux logiciels, programmes informatiques et protocoles permettant de faire fonctionner l'interconnexion entre ces systèmes (couche logique), et qu'aux individus et groupes impliqués dans des activités numériques (couche sociale).

Le commentaire s'arrête aussi sur les différentes qualifications qui ont pu être données au cyberespace et qui auraient potentiellement une incidence sur l'applicabilité du principe de souveraineté. En effet, certains qualifient le cyberespace de patrimoine commun de l'humanité, d'un espace échappant à la souveraineté des États comme la haute mer ou l'espace extra-atmosphérique, ou encore de cinquième domaine pour les activités humaines et militaires. À juste titre, le groupe d'experts rejette ces différentes approches en ce qu'elles ne prennent pas en compte la dimension physique du cyberespace (commentaire sous la règle 1 – §5, p. 12). Le cyberespace repose en effet sur une infrastructure physique qui est soumise à la souveraineté des États et il serait donc contradictoire de considérer que le cyberespace échappe à la souveraineté de ces États.

De la même manière, il n'est pas possible pour les États de revendiquer la souveraineté sur le cyberespace en tant que tel (commentaire sous la règle 1 – §7, p. 13). Ils exercent leur souveraineté sur les infrastructures physiques et par extension au cyberespace qui en dépend, mais la souveraineté sur le domaine fictif que représente le cyberespace ne peut être dissociée de celle sur la couche physique.

Le commentaire aborde une question centrale dans les débats sur la souveraineté dans le cyberspace : est-ce que les États exercent leur souveraineté sur les données gouvernementales ou celles de leurs ressortissants lorsqu'elles sont transmises et stockées à l'étranger ? (commentaire sous la règle 2 – §11, pp. 15-16) La majorité des experts répond par la négative à cette question. Pour eux, les États n'exercent pas leur souveraineté sur leurs données ou celles de leurs ressortissants transmises et stockées à l'étranger, sauf dans des cas où le droit international prévoirait autrement. Une minorité d'experts considère au contraire que les États peuvent exercer leur souveraineté, dans certaines circonstances, sur ces données. Il s'agit ici d'un débat important, tant du point de vue juridique que politique. En effet, l'approche suivie par la majorité des experts semble la plus conforme à la lettre actuelle du droit international. Néanmoins, les données des États et de leurs ressortissants, notamment les données dites stratégiques, représentent un enjeu important et il semble tout à fait imaginable que certains États poussent pour l'adoption de normes, ou à tout le moins de principes non contraignants juridiquement, visant à étendre leur souveraineté sur certaines données pour pouvoir mieux les protéger.

3.2.1.2 Violation de la souveraineté

Les États ne doivent pas mener des cyber opérations qui violeraient la souveraineté d'autres États (**règle 4**). Cette interdiction n'est cependant pas absolue et le droit international prévoit des cas où les États peuvent mener des actions qui devraient normalement constituer une

violation de la souveraineté d'autres États, notamment dans le cadre d'une action autorisée par le Conseil de sécurité des Nations Unies, de la prise de contre-mesures ou de l'exercice du droit de légitime défense (commentaire sous la règle 4 – §1, p. 17).

Le groupe d'experts rappelle qu'il s'agit d'une obligation entre États, **seul un État peut violer la souveraineté d'un autre État** (commentaire sous la règle 4 – §2, p. 17-18). Ainsi, les activités des acteurs privés non attribuables à l'État, et qui relèvent donc de la cybercriminalité, ne peuvent pas être considérées comme des violations de la souveraineté d'un État (commentaire sous la règle 4 – §30, p. 26). Le commentaire note l'existence d'une approche contraire considérant que dans certains cas les activités de groupes d'individus et non attribuables à un Etat pourraient néanmoins violer la souveraineté d'un État, tout en précisant qu'aucun expert du groupe ne partage cette vision (commentaire sous la règle 4 – §3, p. 18). Il note également que la cyber opération n'a pas besoin nécessairement d'émaner du territoire de l'État responsable pour constituer une violation de la souveraineté d'un autre État par cet État, elle peut tout aussi bien être conduite par cet État depuis le territoire d'un autre État ou d'une zone échappant à la souveraineté des États (commentaire sous la règle 4 – §23, p. 24).

Il y a violation de la souveraineté d'un État à partir du moment où un autre État pénètre sur son territoire ou dans son espace aérien sans son consentement ou sans une autre justification découlant du droit international (commentaire sous la règle 4 – §6, p. 19). Par exemple, selon les experts, il y aurait violation de la souveraineté dans le cas de l'organe d'un État présent sur le territoire d'un autre État sans son consentement et qui y conduirait des cyber opérations. Néanmoins, certains experts considèrent qu'il existe une exception dans le cas où il s'agit d'une activité d'espionnage, comme détaillé dans le cinquième chapitre. Cette approche est discutable, et nous reviendrons dessus.

La violation de la souveraineté implique un élément de pénétration sur le territoire de l'autre État, par conséquent l'interception à distance des signaux sans fil hors du territoire de l'État concerné ne constituerait pas une violation de la souveraineté (commentaire sous la règle 4 – §9, p. 19-20). L'action d'interception se déroulant hors du territoire de l'Etat, il n'y a pas de violation de sa souveraineté. Les experts se sont limités à la question des signaux sans fil, mais il convient de souligner qu'il en serait de même pour les données interceptées par un État qui espionnerait des câbles hors du territoire de l'État visé. Ainsi, si un Etat A intercepte des données provenant de l'État B lorsqu'elles transitent dans un câble hors du territoire de l'État B, il n'y aura alors pas de violation de la souveraineté de l'État B par l'Etat A.

La violation de la souveraineté se qualifie indépendamment de la volonté de l'État responsable. Une violation involontaire de la souveraineté d'un autre État, par exemple dans le cadre d'un virus qui se propage de manière incontrôlée, constituerait quand même une violation de la souveraineté du ou des États concernés (commentaire sous la règle 4 – §25, p. 24). De la même manière, il faut qu'il y ait réalisation de la violation pour qu'elle puisse être qualifiée, par exemple une cyber opération qui est interceptée avant de produire ses effets sur le territoire de l'Etat concerné ne constituera pas une violation de sa souveraineté (commentaire sous la règle 4 – §24, p. 24).

3.2.1.2.1 Violation de la souveraineté d'un État par le biais de cyber opérations

Ces différentes considérations nous amènent au cœur de la réflexion, **la violation de la souveraineté d'un État par le biais de cyber opérations conduites par un autre État depuis l'étranger et se déroulant, au moins partiellement, sur son territoire**.

Le groupe d'experts examine la licéité de ces cyber opérations suivant une double grille d'analyse : d'un côté, en analysant la portée de l'atteinte à la souveraineté territoriale de l'État ; d'un autre

côté, en déterminant s'il y a une interférence voire une usurpation de fonctions inhérentes[15] au gouvernement de l'État concerné (commentaire sous la règle 4 – §10, p. 20).

Portée de l'atteinte à la souveraineté territoriale

Pour analyser la portée de l'atteinte à la souveraineté territoriale de l'État concerné, le groupe d'experts identifie trois seuils rangés par ordre décroissant de gravité : la survenance de dommage physique (1), l'altération du fonctionnement (2) et les atteintes se trouvant en dessus de ce dernier seuil (3) (commentaire sous la règle 4 – §11, p. 20).

- En cas dommage physique (§§ 11-12, p. 20). **La majorité des experts considère qu'une cyber opération causant des dommages physiques ou des blessures constitue une violation de la souveraineté**. Une minorité d'experts considérère que ce n'était pas un critère automatique et que, dans certains cas, la survenance de dommages ne serait pas suffisante pour que la cyber opération constitue une violation de la souveraineté.
- En cas d'altération du fonctionnement (§§ 13, p. 20-21). **Une cyber opération qui causerait une altération du fonctionnement d'un système informatique pourrait constituer une violation de la souveraineté si cette altération atteint un certain seuil**. Les experts ne sont néanmoins pas parvenus à trouver un accord permettant de déterminer ce seuil et soulignent qu'il reviendra à la pratique des États de clarifier ces questions. En cas d'altération nécessitant le remplacement ou la réparation de pièces physiques du système informatique, les experts sont d'accord pour considérer qu'il y aurait violation de la souveraineté, puisque cette situation équivaudrait à celle de la survenance de dommages physiques. Certains experts considèrent aussi qu'une cyber opération obligeant à réinstaller le système ou des données essentielles à son fonctionnement, et non simplement de le redémarrer, pourrait aussi être qualifiée de violation de la souveraineté.
- En cas ni de dommage physique ni d'altération du fonctionnement (§§ 14, p. 21), **aucun consensus n'a pu être trouvé parmi les experts pour savoir si ce type de cyber opération pouvait être considéré comme une violation de la souveraineté de l'État concerné**.

Nous analyserons ces différents seuils et l'approche du groupe d'experts en même temps que nous discuterons de la seconde grille d'analyse, l'interférence ou l'usurpation de fonctions inhérentes au gouvernement.

Interférence ou usurpation de fonctions inhérentes au gouvernement

Les experts considèrent qu'une cyber opération qui interfèrerait ou usurperait des fonctions inhérentes au gouvernement d'un État, quelle qu'en soit l'intensité, constituerait une violation de la souveraineté de cet État (commentaire sous la règle 4 – §15, pp. 21-22). Le commentaire ne donne pas de définition de fonctions inhérentes au gouvernement, mais précise néanmoins que le fait qu'elles soient normalement accomplies par les organes de l'Etat ou privatisées n'a pas d'incidence.

---

15 Le *Manuel de Tallinn 2.0* n'offre pas de définition de la notion de « fonctions inhérentes au gouvernement de l'État », le dix-septième paragraphe du commentaire offre quelques exemples : « *The Experts cautioned that under this test, the function in question must be inherently governmental. For example, official communications among a State's leadership are inherently governmental, but when a State posts information on terrorist organisations on a website, the activity, while governmental, is not inherently so because other entities, such as non-governmental organisations, also engage in it. Thus, interference with the former would violate the sovereignty of the target State, whereas interfering with the latter would not. Similarly, a cyber operation that is designed to empty a governmental employee's bank account does not interfere with an inherently governmental function, but one that disrupts the government's ability to pay employee salaries does.* », ainsi que la vingt-sixième note de bas de page: « *In assessing the inherently governmental nature of cyber activities, the International Group of Experts pointed out that the notion of acta jure imperii, used in the context of State immunity, could prove helpful.* ».

En ce qui concerne l'usurpation, le commentaire précise qu'il s'agit de la réalisation de fonctions inhérentes au gouvernement d'un État, sur le territoire de cet État, par un autre État et sans l'autorisation de l'État souverain (commentaire sous la règle 4 – §18, pp. 22-23). Par exemple, il s'agit de l'exécution de fonctions de police sur le territoire d'un État par un autre État sans son consentement. Cette précision du groupe d'experts est particulièrement importante en ce qui concerne les mesures qui peuvent être prises, par exemple, contre un *botnet* sur le territoire d'un autre État.

Concernant l'interférence ou usurpation de fonctions inhérentes au gouvernement, les experts sont partagés sur la question de savoir si l'interférence ou l'usurpation doit se manifester sur le territoire de l'État concerné ou peut aussi se manifester en dehors de son territoire (commentaire sous la règle 4 – §19-20, p. 23). La majorité considère que dès qu'il y a interférence ou usurpation de fonctions inhérentes au gouvernement, il y a violation de la souveraineté de l'État, quel que soit le lieu de manifestation. Ils prennent en exemple le cas de données critiques de l'État stockées à l'étranger, l'interférence avec ces données constituerait une violation de la souveraineté de l'État selon la majorité des experts. L'analyse de cette situation par la majorité des experts peut sembler curieuse puisqu'elle semble en contradiction avec une autre analyse présente dans le *Manuel de Tallinn 2.0*. Dans le commentaire sous la règle 2, il est indiqué que la majorité des experts considère que les États n'exercent pas de souveraineté sur leurs données stockées à l'étranger, même si elles leurs appartiennent ou qu'elles appartiennent à leurs ressortissants (commentaire sous la règle 2 – §11, pp. 15-16). Or, le commentaire sous la règle 4 qui nous intéresse à présent semble suggérer le contraire puisque la majorité des experts considère que l'interférence avec des données critiques de l'État stockées à l'étranger constituerait une violation de la souveraineté de l'État. Cette incohérence souligne la complexité du débat sur les données stratégiques des États et de la question de leur protection.

Analyse de l'approche du *Manuel de Tallinn 2.0*

Nous allons maintenant analyser la double grille d'analyse développée par les experts du *Manuel de Tallinn 2.0* sur la violation de la souveraineté d'un État par le biais de cyber opérations conduites par un autre État depuis l'étranger et se déroulant, au moins partiellement, sur son territoire. D'un côté, ils utilisent comme critère les effets et conséquences de la cyber opération. Elle doit atteindre un certain seuil d'intensité pour pouvoir être qualifiée de violation de la souveraineté. D'un autre côté, ils utilisent le caractère de la cible de la cyber opération comme critère : le fait de viser certaines cibles (les fonctions inhérentes au gouvernement) qualifierait automatiquement une cyber opération de violation de la souveraineté. En résumé, le simple fait qu'une cyber opération se manifeste et produise ses effets sur le territoire de l'État concerné ne suffirait pas, il faudrait qu'elle soit d'une certaine intensité ou qu'elle affecte des cibles bien particulières.

On peut s'interroger sur la pertinence de cette grille d'analyse, en effet, dans le monde physique le simple franchissement de frontière suffit à qualifier la violation de souveraineté, même si cette affirmation peut être tempérée notamment lorsqu'il s'agit d'opérations de police. Par exemple, le fait que l'aéronef militaire d'un État pénètre l'espace aérien d'un autre État est suffisant pour constater la violation de la souveraineté de ce dernier. En serait-il autrement dans le cyberespace ? Le caractère immatériel des cyber opérations rend l'analyse des cyber opérations, et l'analogie avec le monde réel, un peu complexe. Néanmoins, on peut s'interroger sur la pertinence de créer un seuil d'intensité pour la violation de souveraineté.

Ne serait-il pas plus pertinent de considérer que toutes les cyber opérations d'un État produisant ses effets sur territoire d'un autre État constituent une violation de la souveraineté de ce dernier ? Toutes les violations de souveraineté ne se valent pas, l'intensité de la violation ou le caractère de la cible permettrait de déterminer la gravité de la violation et donc les conséquences.

Ainsi, une cyber opération pénétrant dans un système informatique d'un État étranger sans produire ni dommage, ni perte de fonctionnalité et sans que ce système soit lié à une fonction inhérente au gouvernement de cet État constituerait néanmoins une violation de la souveraineté de cet État, certes de faible intensité et l'État concerné ne prendrait probablement pas la peine de relever cette violation. Sur le plan des conséquences, l'État responsable pourrait voir sa responsabilité engagée par l'État concerné, mais de manière assez limitée, d'un côté, si l'État souhaite prendre des contre-mesures elles devront être proportionnées et donc d'une intensité aussi limitée que la cyber opération initiale, d'un autre côté, sur le plan de la réparation, les prétentions de l'État concerné seraient-elles aussi très limitées et il ne pourrait probablement obtenir que la réparation sous forme de satisfaction voire de garantie de non-répétition.

À l'inverse, une cyber opération produisant des dommages physiques constituerait une violation plus grave de la souveraineté de l'État concerné, ouvrant potentiellement la voie à des contre-mesures d'une certaine intensité, et sur le plan de la réparation, l'État concerné pourrait exiger la *restitio in integrum*, qui serait probablement impossible, et donc serait en droit d'exiger la compensation, c'est-à-dire une réparation sous forme pécuniaire.

Il s'agit d'une question assez sensible et que seule la pratique des États permettra de trancher.

3.2.1.2.2 Cyber opérations contre des opérateurs d'importance vitale ou entrainant des pertes économiques significatives

Concernant les cyber opérations contre des opérateurs d'importance vitale ou entrainant des pertes économiques significatives, le groupe d'experts note que rien dans le droit international actuel ne semble aller dans le sens d'un traitement différencié pour les qualifier de violation de la souveraineté. Il note aussi que les États semblent montrer une certaine préférence pour l'approche prenant en compte les effets de ces cyber opérations particulières (commentaire sous la règle 4 – §28, pp. 25-26).

3.2.1.3 Inviolabilité et immunité souveraine

Toute cyber opération d'un État affectant un système d'information installé à bord de plateformes, objets ou appareils bénéficiant d'une immunité souveraine, où qu'ils se trouvent, constitue une violation de souveraineté (**règle 5**). Le commentaire précise que pour bénéficier de cette immunité souveraine, le système d'information concerné doit être dédié exclusivement à des activités gouvernementales (commentaire sous la règle 5 – §2, p. 28).

3.2.2 Obligation de diligence (chapitre 2 – règles 6 et 7)[16]

3.2.2.1 Le contenu de l'obligation de diligence

En droit international, les Etats ont l'obligation « de ne pas laisser utiliser [leur] territoire aux fins d'actes contraires aux droits d'autres États », il s'agit de l'obligation de diligence rappelée par la Cour internationale de justice dans un *dictum* dans son arrêt de 1949 dans l'affaire du *Détroit de*

16 Ian Yuying Liu analyse la mise en œuvre des règles du Manuel de Tallinn 2.0 sur l'obligation de diligence et analyse les raisons de l'opposition de certains Etats à l'application de l'obligation de diligence aux activités numériques. LIU I.Y., « The due diligence doctrine under Tallinn Manual 2.0 », *op. cit.*

Michael N. Schmitt a publié un article où il revient sur les différents points abordés dans les deux éditions du *Manuel de Tallinn* et qui mériteraient d'être étudiés plus en avant, notamment sur l'obligation de diligence et les différents débats qui l'entourent. SCHMITT M.N., « Grey Zones in the International Law of Cyberspace », *op. cit.*, p. 11-13.

Dans le même sens voir aussi : JENSEN E.T., « The Tallinn Manual 2.0 », *op. cit.*, p. 10-13.

Corfou[17]. Le groupe d'experts considère que cette obligation s'applique aussi au contexte numérique (commentaire sous la règle 6 – §4, p. 31), et l'a transposé dans la **règle 6** : **Un État doit exercer son devoir de diligence en ne permettant pas l'utilisation de son territoire, d'un territoire ou d'un système d'information sur lequel il exerce son contrôle gouvernemental, pour la conduite de cyber opérations contraire aux droits d'autres États et les affectant avec des conséquences graves**.

L'applicabilité du principe de diligence due dans le contexte numérique a aussi été affirmée par le GGE[18]. A noter que le GGE adopte une interprétation assez restrictive de l'obligation de diligence. Il convient de distinguer la diligence due d'autres obligations de prévention existantes en droit international, comme l'obligation de prévention du crime de génocide[19] (commentaire sous la règle 6 – §6, p. 32).

Le commentaire rappelle qu'il s'agit d'une situation à trois parties :

- L'État victime ;
- L'État sur qui pèse l'obligation : c'est-à-dire celui depuis le territoire duquel est utilisé, ou qui exerce son contrôle sur le territoire ou les infrastructures utilisés ;
- Le tiers conduisant la cyber opération, il peut s'agir d'un État ou d'un acteur non étatique.

Il convient de distinguer l'État depuis le territoire duquel une cyber opération est lancée, de celui sur le territoire duquel elle transite notamment en passant par des câbles situés sur son territoire.

Le groupe d'experts considère que l'obligation de diligence s'applique aussi à l'État de transit lorsque deux conditions cumulatives sont remplies : premièrement, lorsque l'État connait ou devrait connaitre l'existence de l'opération atteignant un certain seuil d'intensité ; deuxièmement, lorsqu'il est en capacité de prendre des mesures pour y mettre un terme (commentaire sous la règle 6 – §13, p. 33). Néanmoins, les experts notent que dans l'état actuel des connaissances il serait difficile pour un État d'identifier le trafic relatif à ces cyber opérations malveillantes (commentaire sous la règle 6 – §14, p. 34).

Concernant les conséquences des cyber opérations, le groupe d'experts considère qu'il y a deux critères cumulatifs : d'un côté, la cyber opération doit être contraire aux droits d'autres États et, d'un autre côté, elle doit les affecter avec des conséquences graves (commentaire sous la règle 6 – §15, p. 34). En effet, **l'obligation de diligence ne s'applique que lorsque l'acte en question constitue un acte internationalement illicite ou constituerait un acte internationalement illicite s'il était attribuable à un État, notamment celui dont le territoire duquel est utilisé pour le perpétrer** (commentaire sous la règle 6 – §15-24, pp. 34-36). Un acte qui produirait des conséquences graves sans pour autant violer les droits de l'État concerné ne pourrait pas servir de base à l'obligation de diligence. Dans le même sens, le lieu où se produisent les conséquences de la cyber opération, sur le territoire de l'État victime ou à l'étranger, ou la nature privée ou publique de la cible, n'ont pas d'incidence sur l'obligation de diligence, tout ce qui compte c'est qu'il y ait une atteinte au droit de l'État victime (commentaire sous la règle 6 – §§33,36, pp. 39-40).

Le second critère est un seuil d'intensité, seules les cyber opérations ayant des conséquences graves peuvent servir de base à l'obligation de diligence. Les experts soulignent que ce seuil n'est aujourd'hui pas clairement identifié en droit international (commentaire sous la règle 6 – §25,

---

17 *Détroit de Corfou (Royaume-Uni de Grande-Bretagne et d'Irlande du Nord c. Albanie)* (Arrêt sur le fond), 1949, p. 22.

18 *Rapport 2013 du GGE*, *op. cit.*, para 23 ; *Rapport 2015 du GGE*, *op. cit.*, para 13(c).

19 Convention pour la prévention et la répression du crime de génocide, adoptée le 9 décembre 1948 en entrée en vigueur le 12 janvier 1952, Nations Unies, *Recueil des traités*, Vol. 78, p.277.

pp. 36-37). Ils précisent avoir créé ce seuil d'intensité minimal par analogie avec le droit international de l'environnement. Cependant, certains experts étaient en faveur d'un seuil bien moins élevé. Ce seuil d'intensité minimal sert à exclure les opérations ayant les conséquences négatives les moins graves, voire négligeables. À l'inverse, il précise que l'occurrence de dommage physique ou de blessures n'est pas requise pour que ce seuil soit atteint (commentaire sous la règle 6 – §§26-28, pp. 37-38). À notre avis, les raisons avancées par le groupe d'experts pour soutenir la création d'une exigence d'intensité sont pertinentes. **Néanmoins, de notre avis, il serait possible de considérer qu'il n'y a pas de seuil d'intensité pour la qualification de la violation de l'obligation de diligence, mais que comme nous l'avons proposé dans le cadre de la violation de souveraineté, l'intensité de l'acte servirait à déterminer la gravité de la violation et donc l'étendue de ses conséquences.**

Le groupe d'experts est divisé sur le cas particulier des *botnets*. L'exemple donné est celui d'une opération transitant par un *botnet* installé sur le territoire de plusieurs États et produisant des conséquences graves. Prises séparément, les opérations transitant par le territoire de chaque État n'auraient pas à elles seules des conséquences graves, mais c'est leur somme qui augmenterait la gravité des conséquences. Est-ce que les Etats sur les territoires desquels le *botnet* est localisé ont une obligation de diligence de prendre des mesures pour mettre un terme à ce *botnet* et cette opération ? La majorité des experts considère que les États sur le territoire desquels s'étend le *botnet* n'ont pas une obligation de diligence relative à toutes les conséquences de l'action menée par le *botnet*. Chaque État n'est concerné que par la portion de l'opération qui transite par son territoire. De notre avis, il s'agit là d'une question sensible et qui rejoint notre analyse faite précédemment sur l'existence d'un seuil d'intensité.

L'obligation de diligence s'applique lorsque l'État dont le territoire est utilisé connait ou devrait connaitre l'existence de l'opération affectant les droits de l'autre État. La connaissance de l'État du territoire concerné peut découler d'une notification de la part de l'État affecté. Il peut être difficile pour l'État affecté de prouver la connaissance de l'État du territoire concerné, mais si les circonstances font que cet État devrait être au courant alors l'obligation de diligence peut s'appliquer (commentaire sous la règle 6 – §§37-42, pp. 40-42). Il faut distinguer le standard de préemption de connaissance de l'existence de l'opération d'une obligation de prévention ; en effet, il n'existe pas d'obligation de prévention (commentaire sous la règle 6 – §42, pp. 41-42).

Il est aussi important de **distinguer le non-respect de l'obligation de diligence de l'assistance que pourrait apporter un État à la commission d'un acte internationalement illicite** (commentaire sous la règle 6 – §43, p. 42).

3.2.2.2 Mise en œuvre de l'obligation de diligence

La **règle 7** détaille la mise en œuvre de l'obligation de diligence. **L'obligation de diligence impose aux États de prendre toutes les mesures possibles pour mettre un terme aux cyber opérations contraire aux droits d'un autre État et l'affectant avec des conséquences graves**.

Ainsi, **l'obligation de diligence est une obligation de moyen et non une obligation de résultat**. L'État sera reconnu responsable de non-conformité avec cette obligation s'il ne prend pas les mesures nécessaires ou si les mesures prises sont insuffisantes, mais pas parce que l'acte s'est déroulé.

La majorité des experts considère que cette obligation s'étend aux opérations qui n'ont pas encore été mises en œuvre, mais qui sont imminentes (commentaire sous la règle 7 – §3, pp. 43).

Le choix des mesures mises en œuvre reste à la discrétion de l'État du territoire concerné (commentaire sous la règle 7 – §6, p. 44). L'État n'est pas tenu à l'impossible, il doit mettre en œuvre toutes les mesures nécessaires, mais possibles pour mettre un terme à l'opération, sans que cela représente un fardeau impossible pour lui (commentaire sous la règle 7 – §§16-17, p. 47). Les mesures que doit prendre l'État doivent aussi être raisonnables, c'est-à-dire qu'elles ne doivent pas imposer un fardeau trop important et disproportionné au regard du résultat espéré (commentaire sous la règle 7 – §25, pp. 49-50). **La liberté de choix des mesures s'étend aussi à leurs auteurs, il peut s'agir des organes de l'Etat ou d'acteurs non étatiques agissant pour le compte de l'État**. Si le système d'information utilisé dépend d'une entité privée qui refuse de coopérer avec l'État du territoire concerné, ce dernier ne pourra pas s'en prévaloir et devra mettre en œuvre les mesures nécessaires pour obliger l'acteur non étatique à coopérer (commentaire sous la règle 7 – §20, p. 48). Les Etats n'ont pas d'obligation d'adopter préventivement les mesures législatives leur permettant de respecter leurs possibles futures obligations de diligence, mais ils ne peuvent pas non plus se prévaloir de leur droit national comme circonstance justifiant le non-respect de leur obligation (commentaire sous la règle 7 – §§21-22, pp. 48-49). L'État du territoire concerné n'est pas non plus obligé de demander l'assistance d'autres États dans la mise en œuvre de son obligation de diligence (commentaire sous la règle 7 – §26, p. 50). Il convient ici de souligner que les rapports adoptés en 2013 et 2015 par le Groupe d'experts gouvernementaux des Nations Unies encouragent les Etats à mettre en place un certain nombre de bonnes pratiques et à adopter des législations visant à lutter contre la cyber criminalité.

Comme noté précédemment, **l'obligation de diligence n'implique pas d'obligation de prévention** (commentaire sous la règle 7 – §§7-13, pp. 44-46). De plus, **le groupe d'experts considère qu'une telle obligation de prévention serait très difficile à mettre en œuvre sur le plan pratique et ferait peser sur l'État du territoire concerné un poids insoutenable** (§ 8, p. 45). N'impliquant pas d'obligation de prévention, **l'obligation de diligence n'impose pas non plus une obligation générale pour les États de surveiller les activités numériques se déroulant sur leur territoire** (§ 10, pp. 45). Ainsi, les Etats ne peuvent pas utiliser l'obligation de diligence comme justification pour d'éventuelles violations du droit international, par exemple, la violation des droits de l'homme résultant de la mise en place d'un programme de surveillance de masse. Il s'agit d'une précision importante puisque l'obligation de diligence pourrait être utilisée par certains États pour justifier la mise en place de programme de surveillance globale des activités numériques de leurs citoyens.

L'État qui ne respecterait pas son obligation de diligence, c'est-à-dire qui ne mettrait pas en œuvre les mesures nécessaires malgré sa capacité à prendre ces mesures, pourrait voir sa responsabilité internationale engagée. En outre, l'État victime pourrait avoir recours à des contre-mesures pour l'obliger à se conformer à son obligation de diligence (commentaire sous la règle 7 – §28, p. 50).

3.2.3 Compétences de l'État (*jurisdiction*) (chapitre 3 – règles 8 à 13)

Le troisième chapitre du *Manuel de Tallinn 2.0* analyse les compétences exercées par les États sur le cyberespace et les activités numériques. Ainsi, **l'État exerce sa compétence territoriale et extraterritoriale sur les activités numériques dans les conditions posées par le droit international** (**règle 8**).

Il convient de distinguer la compétence territoriale de la compétence extraterritoriale de l'État.

- **L'Etat exerce sa compétence territoriale sur les personnes, objets et systèmes d'information situés sur son territoire, les cyber opérations lancées ou se déroulant partiellement sur son territoire, ou sur les cyber opérations ayant des effets sur son**

territoire (**règle 9** ; commentaire sous la règle 8 – §4, p. 51). Sur son territoire l'État exerce pleinement ses compétences normatives, exécutives et judiciaires (commentaire sous la règle 8 – §3, pp. 51-52).

- **En dehors de son territoire, l'État peut exercer sa compétence extraterritoriale** :
  - L'État peut exercer sa compétence normative extraterritoriale pour les cyber opérations conduites par ses nationaux, perpétrées sur des navires ou aéronefs ayant sa nationalité, conduites par des ressortissants étrangers et visant à nuire gravement aux intérêts de l'État, contre ses nationaux ou si elles constituent un crime international de compétence universelle (**règle 10**).
  - L'État peut exercer sa compétence judiciaire extraterritoriale sur les personnes, objets et cyber opérations s'il dispose d'un titre en ce sens aux termes du droit international ou si l'État ayant la compétence territoriale consent à ce qu'il exerce sa compétence judiciaire extraterritoriale (**règle 11**).

Nous ne détaillerons pas ici la discussion générale sur les compétences de l'État.

L'analyse des compétences de l'État nous conduit à nous intéresser aux immunités de juridiction dont bénéficient les États en droit international. Ainsi, **l'immunité de juridiction dont bénéficient certaines personnes, objets ou avoirs s'applique aussi aux activités numériques et aux systèmes d'information** (**règle 12**).

Les États sont libres de coopérer ou non avec d'autres États, notamment lorsqu'il s'agit de poursuivre des cyber crimes, néanmoins certains traités internationaux ou obligations internationales peuvent imposer aux États de coopérer (**règle 13**). Ainsi, les experts notent qu'il n'existe aucune règle de droit coutumier imposant aux États de coopérer (commentaire sous la règle 13 – §1, p. 75). Il convient de souligner les efforts des Etats en ce sens, notamment avec l'adoption par le Groupe d'experts gouvernementaux des Nations Unies de la norme 13(h) du rapport de 2015 et les efforts entrepris au sein de l'OSCE.

3.2.4 Droit de la responsabilité internationale (chapitre 4 – règles 14 à 31)

Les trois premières sections sont dédiées à la responsabilité internationale des États et sont dans une large proportion basées sur les Articles sur la responsabilité de l'État pour fait internationalement illicite adoptés par la Commission du droit international des Nations Unies (CDI) en 2001 et qui reflètent le droit coutumier international. Le groupe considère néanmoins que certaines questions n'ont pas été entièrement résolues par les Articles de la CDI sur la responsabilité de l'État ou que certains articles ne sont pas considérés comme reflétant la coutume internationale par tous les États (commentaire introductif du chapitre 4 – §1, p. 79).

Les experts notent qu'il n'existe pas d'obligation en droit international, pour un État réagissant à l'acte internationalement illicite d'un autre État, d'apporter publiquement la preuve de l'imputabilité de l'acte en question à l'État responsable (commentaire introductif du chapitre 4 – §13, p. 83). Ils notent néanmoins que produire publiquement ces éléments au moment de réagir permet de limiter les tensions et le risque d'escalade entre les États concernés. Ils soulignent aussi que certains États semblent avoir adopté des positions en faveur de la production publique de ces preuves au moment de réagir, sans pouvoir identifier une *opinio juris* et une pratique suffisante qui impliqueraient une évolution du droit existant. Néanmoins, la production de preuve est de plus en plus encouragée afin de justifier les actions entreprises. Dans le domaine numérique, le paragraphe 28(f) du rapport de 2015 du Groupe d'experts gouvernementaux des Nations Unies souligne que « *le Groupe a fait observer que les accusations d'organiser et d'exécuter des actes illicites portées contre des États devaient être étayées* ».

3.2.4.1 Faits internationalement illicites d'un État (Chapitre 4, section 1 – règles 14 à 19)

3.2.4.1.1 Définition du fait internationalement illicite d'un État

Un État est internationalement responsable pour les activités à dimension numérique qui lui sont attribuables et qui constituent une violation d'une obligation internationale de cet État (**règle 14**). En d'autres termes, la responsabilité internationale d'un État dépend de deux critères cumulatifs : premièrement, que l'acte lui soit attribuable ; deuxièmement, que cet acte constitue une violation d'une obligation internationale de l'État.

Le fait internationalement illicite de l'État peut être le résultat d'une action, mais aussi d'une omission de la part de cet État (commentaire sous la règle 14 – §5, p. 85).

L'État sera responsable si le fait lui est attribuable et qu'il constitue une violation d'une obligation internationale, qu'il résulte dans la survenance de dommage ou non (commentaire sous la règle 14 – §§ 6-8, pp. 85-86). Il convient d'ajouter ici qu'à l'inverse, l'État ne sera pas responsable internationalement en cas de dommage résultant d'un fait qui ne serait pas internationalement illicite, même s'il convient de noter le développement de régimes de responsabilité sans violation du droit international, notamment dans le cadre du droit de l'environnement.

3.2.4.1.2 Attribution

Les règles 15 à 18 traitent de la question de l'attribution d'une cyber opération à un État[20].

[20] William C. Banks, dans un article préparé dans le cadre du *Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* fait une analyse sommaire des règles du *Manuel de Tallinn 2.0* sur l'attribution et les met en pratique au regard du piratage du Parti Démocrate durant la campagne présidentielle américaine de 2016. BANKS W.C., « State Responsibility and Attribution of Cyber Intrusions after *Tallinn 2.0* [*Symposium:* Tallinn Manual 2.0 *on the International Law Applicable to Cyber Operations*] », *Texas Law Review*, 2017 2016, vol. 95, p. 1487‑1513.

Les cyber opérations conduites par un organe de l'État ou par une personne ou une entité exerçant des prérogatives de puissance publique sont attribuables à l'État (**règle 15**). Le commentaire souligne que ce serait par exemple le cas des activités numériques de l'US Cyber Command, le Defence Cyber Command des Pays-Bas et de l'Agence nationale de sécurité des systèmes d'information (ANSSI) (commentaire sous la règle 15 – §1, p. 87). Par ailleurs, l'État est responsable même si l'acte est *ultra vires*, c'est-à-dire même si l'organe de l'État, la personne ou l'entité exerçant des prérogatives de puissance publique agissant en cette qualité outrepasse sa compétence ou contrevient à ses instructions (commentaire sous la règle 15 – §6, p. 89). L'État ne sera pas responsable s'il s'agit d'un acte ou d'une omission purement privés.

Les cyber opérations conduites par l'organe d'un État mis à la disposition d'un autre État sont attribuables à ce dernier lorsque l'organe exerce des prérogatives de puissance publique de l'État à la disposition duquel il se trouve (**règle 16**). Cette règle s'applique aussi aux actes *ultra vires* (commentaire sous la règle 16 – §5, p. 94).

La **règle 17** concerne **l'attribution d'actes, et donc de cyber opérations, menés par des acteurs non étatiques**. Elle identifie deux situations distinctes dans lesquelles ces actes sont attribuables à l'État : d'un côté, **lorsqu'ils sont menés si la personne ou le groupe de personnes agit en fait sur ses instructions ou ses directives ou sous son contrôle** (**règle 17*a***) ; d'un autre côté, **lorsque l'État reconnaît et adopte ces actes comme les siens** (**règle 17*b***). Cette règle appelle plusieurs remarques.

La règle 17*a* reprend l'article 8 des Articles de la CDI sur la responsabilité de l'État. Le commentaire souligne que la Cour internationale de justice, dans les affaires *Nicaragua* et *Génocide*, adopte une approche différente de celle de la CDI. En effet, la CDI considère que les critères de 'contrôle', 'instructions' et 'directives' sont indépendants alors que la CIJ traite les critères de 'directives' et de 'contrôle' ensemble en ayant recours au test du 'contrôle effectif'. Il convient aussi de distinguer le critère du 'contrôle global' développé par le Tribunal pénal pour l'ex-Yougoslavie dans l'affaire *Tadić* pour déterminer la nature des conflits armés, ce que rappelle le commentaire (§ 6, p. 96), qui aurait néanmoins pu être analysé puisqu'il s'agissait aussi de déterminer l'attribution d'actes même si la finalité de cette attribution était différente. Le commentaire tend à assimiler l'approche de la CIJ de celle de la CDI : « *In the commentary to the Articles on State Responsibility, the International Law Commission indicated that the terms 'instruction', 'direction', and 'control' are to be understood in the disjunctive. However, courts tend to treat 'direction' and 'control' together. The two terms refer to a continuing process of exercising authority over an activity such as a cyber operation. The International Group of Experts agreed that the phrase 'effective control' employed by the International Court of Justice in the Nicaragua and Genocide judgements captures the scope of the concept.* » (notes de bas de page non reprises – commentaire sous la règle 17 – §5, p. 96) Deux remarques : d'une part, même si les standards utilisés par la CIJ et la CDI sont très proches, ils sont néanmoins distincts et celui utilisé par la CIJ est plus restrictif que celui de la CDI ; d'autre part, il aurait été souhaitable d'avoir une analyse plus poussée des différents standards et de leurs implications[21]. L'articulation entre ces différentes approches amène le lecteur à s'interroger sur la pertinence d'un possible assouplissement de ces critères dans le domaine numérique, néanmoins cette réflexion sort du cadre de cette analyse.

Les actes *ultra vires* des acteurs non étatiques ne peuvent pas être attribués aux États (commentaire sous la règle 17 – §§11-14, pp. 97-99). En effet, il s'agit d'une analyse acte par acte,

21 Michael N. Schmitt a publié un article où il revient sur les différents points abordés dans les deux éditions du *Manuel de Tallinn* et qui mériteraient d'être étudiés plus en avant, il revient notamment sur l'attribution et plus précisément sur les différents seuils pour l'attribution à un Etat des actes de groupes non-étatiques. SCHMITT M.N., « Grey Zones in the International Law of Cyberspace », *op. cit.*, p. 8-10.

et seuls les actes conduit sous la direction, le contrôle ou les instructions de l'État pourront lui être attribués.

La règle 17*b* est basée sur l'article 11 des Articles de la CDI sur la responsabilité de l'État. Un État peut reconnaître et adopter des actes comme les siens, même s'ils ne lui sont pas attribuables. Dans ce cas, les actes seront considérés comme des actes de l'État. Il convient de souligner que pour être attribuable, l'acte doit à la fois être 'reconnu' et 'adopté' par l'État, il s'agit de deux critères cumulatifs.

La règle 17 reprend deux articles de la CDI sur l'attribution d'actes d'acteurs non étatiques, d'un côté l'article 8 concernant les comportements exécutés sous la direction ou le contrôle de l'État, et de l'autre côté, l'article 11 concernant les comportements reconnus et adoptés par l'État comme étant siens. Les Articles de la CDI sur la responsabilité de l'État donnent deux bases supplémentaires d'attribution des actes d'acteurs non étatique qui ne sont pas reprises ni dans la règle 17 ni dans son commentaire :

- L'article 9 prévoit les conditions d'**attribution d'un comportement en cas d'absence ou de carence des autorités officielles de l'État**, cette disposition est néanmoins brièvement évoquée dans le commentaire sous la règle 15 sur les organes de l'État (§ 17, p. 92) ;

  > **Article 9 des Articles de la CDI** – *Comportement en cas d'absence ou de carence des autorités officielles* :
  >
  > « *Le comportement d'une personne ou d'un groupe de personnes est considéré comme un fait de l'État d'après le droit international si cette* personne *ou ce groupe de personnes exerce en fait des prérogatives de puissance publique en cas d'absence ou de carence des autorités officielles et dans des circonstances qui requièrent l'exercice de ces prérogatives.* »

- L'article 10 prévoit les conditions d'**attribution d'un comportement d'un mouvement insurrectionnel** et n'est pas repris dans le Manuel.

  > **Article 10 des Articles de la CDI** – *Comportement d'un mouvement insurrectionnel ou autre* :
  >
  > « 1. Le comportement d'un mouvement insurrectionnel qui devient le nouveau gouvernement de l'État est considéré comme un fait de cet État d'après le droit international.
  >
  > 2. Le comportement d'un mouvement insurrectionnel ou autre qui parvient à créer un nouvel État sur une partie du territoire d'un État préexistant ou sur un territoire sous son administration est considéré comme un fait de ce nouvel État d'après le droit international.
  >
  > 3. Le présent article est sans préjudice de l'attribution à l'État de tout comportement, lié de quelque façon que ce soit à celui du mouvement concerné, qui doit être considéré comme un fait de cet État en vertu des articles 4 à 9. »

Ces deux bases pour l'attribution d'actes d'acteurs non étatiques sont certes de moindre importance que les deux précédentes, mais ne doivent néanmoins pas être ignorées. En effet, les récentes situations de guerres civiles voire de déliquescence de certains États soulignent l'importance de s'intéresser à ce type de situations. D'autant que de nombreux groupes non étatiques, qu'il s'agisse de mouvements insurrectionnels ou de groupes terroristes, maîtrisent dans des degrés divers l'utilisation des nouvelles technologies et conduisent des cyber opérations.

3.2.4.1.3 Responsabilité de l'État à raison des cyber opérations d'autres États

La règle 18 sur la responsabilité à raison des cyber opérations conduites par d'autres États reprend les articles 16 à 18 des Articles de la CDI sur la responsabilité de l'État, les trois alinéas de la règle paraphrasant les trois articles de la CDI.

Ainsi, aux termes de la **règle 18** relative aux **cyber opérations conduites par d'autres États, un État sera considéré responsable** :

- **de l'aide ou l'assistance apportée à un autre État dans la commission du fait internationalement illicite**, dans le cas où il agit ainsi en connaissance des circonstances du fait internationalement illicite et que le fait serait internationalement illicite s'il était commis par cet État.
- **de l'acte internationalement illicite d'un autre État pour lequel il a donné des directives et a exercé un contrôle dans la commission du fait internationalement illicite par l'autre État**, dans le cas où il agit ainsi en connaissance des circonstances du fait internationalement illicite et que le fait serait internationalement illicite s'il était commis par cet État.
- **de l'acte internationalement illicite d'un autre État qu'il aurait contraint à commettre cet acte**.

Une distinction importante entre les trois situations : un État qui apporte son aide ou son assistance ne sera responsable que de son aide ou son assistance, et non de l'acte internationalement illicite lui-même, à l'inverse des cas où l'État donne des directives et contrôle la commission de l'acte ou contraint l'autre État à le commettre (commentaire sous la règle 18 – § 6, p. 102).

3.2.4.1.4 Circonstances excluant l'illicéité

La **règle 19** reprend les six circonstances excluant l'illicéité d'un acte internationalement illicite listées aux articles 20 à 25 des Articles de la CDI sur la responsabilité de l'État. Ainsi, **l'illicéité d'un acte impliquant des cyber opérations est exclue s'il s'agit d'une situation de :**

- **Consentement ;**
- **Légitime défense ;**
- **Contre-mesures ;**
- **Nécessité ;**
- **Force majeure ;**
- **Détresse.**

Il convient de souligner que la règle 19 ne traite que des situations dans lesquelles l'illicéité d'une cyber opération serait exclue par des circonstances particulières, il ne s'agit pas ici d'analyser les situations où des cyber opérations seraient responsables de la survenance d'une circonstance excluant l'illicéité.

Trois circonstances font l'objet de règles et de commentaires dans d'autres parties du *Manuel*, il s'agit de la légitime défense (règles 71-75), des contre-mesures (règles 20-25) et de la nécessité (règle 26).

Dans le cadre du **consentement** de l'État, l'illicéité ne sera exclue que si le consentement est valide, notamment du point de vue du droit, et que l'acte reste dans les limites de ce consentement (commentaire sous la règle 19 – §3, pp. 104-105). **Le consentement peut être donné de manière express ou implicite, mais il doit néanmoins toujours être donné avant que survienne l'acte ou l'omission en question** (commentaire sous la règle 19 – §§7-8, p. 106). Le consentement est valide s'il est donné par une autorité compétente de l'État, néanmoins si

l'État a reçu le consentement d'une autorité n'ayant pas la capacité de le donner, mais qu'il agit de bonne foi, c'est-à-dire sans savoir que l'autorité ayant donné le consentement est incompétente, alors l'illicéité de l'acte pourra quand même être exclue (commentaire sous la règle 19 – §§4-6, pp. 105-106).

La **force majeure** consiste *« en la survenance d'une force irrésistible ou d'un événement extérieur imprévu qui échappe au contrôle de l'État et fait qu'il est matériellement impossible, étant donné les circonstances, d'exécuter l'obligation »* aux termes de l'article 23(1) des Articles de la CDI sur la responsabilité de l'État, repris dans le commentaire (§ 15, p. 108). L'État ne doit pas être à l'origine, pour tout ou partie, de la situation de force majeure. Le commentaire aurait pu aller plus loin en soulignant la distinction entre force majeure et nécessité : d'un côté, l'État n'a pas d'autres possibilités (force majeure), alors que de l'autre côté, l'État doit agir, mais garde une certaine liberté dans le choix des moyens employés (nécessité). Ce faisant, il aurait alors été utile pour le commentaire de souligner qu'il semble hautement improbable d'avoir une situation de force majeure justifiant le recours à une cyber opération. En effet, la force majeure sert principalement à exclure l'illicéité du non-respect d'une obligation par omission que par la conduite d'une action, puisque cela implique généralement une marge de choix de la part de l'État.

La **détresse** se distingue des autres circonstances excluant l'illicéité puisqu'elle s'intéresse à la situation de l'auteur de l'acte ou d'autres personnes. Il s'agit en effet du cas où *« l'auteur dudit fait n'a raisonnablement pas d'autre moyen, dans une situation de détresse, de sauver sa propre vie ou celle de personnes qu'il a la charge de protéger »* aux termes de l'article 24(1) des Articles de la CDI sur la responsabilité de l'État, repris par le commentaire (§ 18, pp. 109-110). Comme pour la force majeure, la détresse ne pourra pas être invoquée si l'État est à l'origine, pour tout ou partie, de la situation de détresse (commentaire sous la règle 19 – §20, p. 110). De plus, elle ne pourra pas être invoquée si l'acte est *« susceptible de créer un péril comparable ou plus grave »* (article 24(2)(b) des Articles de la CDI sur la responsabilité de l'État, repris par le commentaire : § 20, p. 110).

Les deux derniers paragraphes du commentaire sous la règle 19 soulignent deux particularités. D'un côté, les opérations autorisées par le Conseil de sécurité des Nations Unies aux termes du Chapitre VII de la Charte des Nations Unies sont licites *ab initio* et ne sont donc pas concernées (§ 21, p. 110). D'un autre côté, l'illicéité liée à la violation d'une règle impérative du droit international général ne peut être en aucun cas exclue par une circonstance particulière (article 26 des Articles de la CDI sur la responsabilité de l'État, repris par le commentaire § 22, p. 110).

3.2.4.2 Contre-mesures (Chapitre 4, section 2 – règles 20 à 25)

La seconde section du quatrième chapitre traite conjointement des contre-mesures et de l'état de nécessité, il nous est apparu nécessaire de les traiter séparément.

Les contre-mesures apparaissent à deux endroits distincts dans les Articles de la CDI sur la responsabilité de l'État, d'abord avec l'article 22 au sein du chapitre sur les circonstances excluant l'illicéité, puis dans le second chapitre de la troisième partie. En effet, un chapitre, comportant six articles, est spécifiquement dédié aux contre-mesures (articles 49 à 54). Les six règles du *Manuel de Tallinn 2.0* sur les contre-mesures s'inspirent fortement des Articles de la CDI sur la responsabilité de l'État.

Avant d'analyser le contenu du *Manuel de Tallinn 2.0* sur les contre-mesures[22], il convient d'ajouter ici, dans un souci de précision et de clarté, que les contre-mesures sont l'une des trois formes de

[22] Dans son article sur les règles sur l'attribution contenues dans le *Manuel de Tallinn 2.0*, William C. Banks traite aussi de la question des contre-mesures au regard de la réponse américaine au piratage du Parti Démocrate durant la campagne présidentielle américaine de 2016. BANKS W.C., « State Responsibility and Attribution of Cyber Intrusions after *Tallinn 2.0* », *op. cit.*, p. 1501‑1505.

mesures unilatérales extrajudiciaires que peuvent adopter les États en réaction à un acte ou une omission d'un autre État. Les deux autres étant la légitime défense et les mesures de rétorsion. Cette dernière forme de mesures unilatérales extraterritoriales est absente du *Manuel de Tallinn 2.0*.

De manière générale, **un Etat lésé peut prendre des contre-mesures, de nature numérique ou non, en réaction à la violation d'une obligation internationale par un autre Etat** : « *A State may be entitled to takes countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another State.* » (**règle 20**). **Seulement possibles en réaction à un acte internationalement illicite, les contre-mesures sont des actions ou des omissions de l'État lésé à l'encontre de l'État responsable qui constitueraient normalement une violation d'une obligation de l'État lésé envers l'État responsable**.

Les contre-mesures doivent être pacifiques, c'est-à-dire qu'elles ne doivent pas porter atteinte à l'obligation de ne pas recourir à la menace ou à l'emploi de la force telle qu'elle est énoncée dans la Charte des Nations Unies (article 50(1)(a) des articles de la CDI, repris dans le commentaire sous la règle 20 – §2, pp. 111-112). Certains considèrent néanmoins que, sous certaines conditions, les États pourraient avoir recours à des contre-mesures armées, comme nous le verrons plus en avant dans cette note.

L'État responsable doit être l'objet des contre-mesures, puisque leur objectif doit être de l'amener à s'acquitter des obligations qui lui incombent, ce qui n'empêche en rien qu'elles soient dirigées contre des acteurs et infrastructures non étatiques (commentaire sous la règle 20 – §6, pp. 112-113). Il convient de noter qu'un État ne peut adopter des contre-mesures qu'à l'encontre d'un autre État pour un fait internationalement illicite de cet État, **il n'existe pas de droit de contre-mesures contre des acteurs non étatiques**. Le groupe d'experts souligne néanmoins l'existence d'un courant doctrinal considérant comme valides les contre-mesures à l'encontre d'acteurs non étatiques (commentaire sous la règle 20 – §§8-9, pp. 113-114). Par ailleurs, **les acteurs non étatiques ne peuvent pas mener de contre-mesures, sauf s'ils agissent pour le compte d'un État, car il s'agit d'un droit exclusivement étatique**.

Comme souligné précédemment à propos des circonstances excluant l'illicéité, les opérations autorisées par le Conseil de sécurité des Nations Unies aux termes du Chapitre VII de la Charte des Nations Unies sont licites *ab initio* et ne sont donc pas considérées comme des contre-mesures (commentaire sous la règle 20 – §11, p. 114).

L'objet des contre-mesures est défini par la règle 21, qui reprend l'article 49(1) des Articles de la CDI sur la responsabilité de l'État. Ainsi, **les contre-mesures, de nature numérique ou non, ne peuvent être prises que pour amener l'État responsable à s'acquitter des obligations qui lui incombent envers l'État lésé** (**règle 21**) et non pour mener des actions punitives. En d'autres termes, des contre-mesures peuvent être prises pour amener l'État responsable à :

- mettre fin au fait internationalement illicite si ce fait continue ;
- accorder une réparation à l'État lésé, voire d'offrir des assurances et des garanties de non-répétition appropriées si les circonstances l'exigent[23].

Ces deux objectifs sont indépendants l'un de l'autre : un État peut prendre des contre-mesures contre un fait internationalement illicite qui a pris fin, mais qui n'a pas encore été réparé par l'État responsable. Un État ne peut pas prendre de contre-mesures, ou doit y mettre un terme, si l'État responsable a cessé l'acte internationalement illicite et accordé les formes appropriées de réparation.

---

[23] Il s'agit ici d'une des différences principales entre les contre-mesures et la légitime défense, en effet, les mesures de légitime défense doivent prendre fin avec la fin de l'acte internationalement illicite alors que les contre-mesures peuvent perdurer jusqu'à l'obtention de la réparation.

Le groupe d'experts était divisé sur la question de savoir s'il existe une obligation pour l'État lésé de prendre des mesures de moindre intensité, par exemple des mesures de rétorsion, pour convaincre l'État responsable de mettre fin à son acte internationalement illicite avant d'avoir recours à des contre-mesures (commentaire sous la règle 21 – §4, pp. 117-118). La majorité des experts considère qu'une telle obligation n'existe pas et que l'objectif de limiter le risque d'escalade lié aux contre-mesures est déjà rempli par l'obligation de notifier la prise de contre-mesures avant leur commencement.

Les contre-mesures ne peuvent être adoptées que contre un acte internationalement illicite qui s'est matérialisé, il n'est pas possible de prendre des contre-mesures contre un acte imminent, mais qui n'a pas encore commencé ou de manière préventive (commentaire sous la règle 21 – §5, p. 118)[24].

L'article 49(3) des Articles de la CDI sur la responsabilité de l'État précise que *« [l]es contre-mesures doivent, autant que possible, être prises d'une manière qui permette la reprise de l'exécution des obligations en question »*. Il est intéressant de noter que cette limitation importante dans le choix et la conduite des contre-mesures n'a pas été reprise dans les règles du *Manuel de Tallinn 2.0* et est seulement mentionnée dans le commentaire sous la règle 20 (§8 – p. 119). Comme l'implique le texte de l'article 49(3) et le précise le commentaire du *Manuel de Tallinn*, l'obligation de réversibilité n'est pas absolue.

Le groupe d'experts n'a pas réussi à s'accorder sur la question de savoir si l'État doit choisir la forme de contre-mesures possibles offrant la meilleure réversibilité ou simplement une forme qui soit réversible. La majorité des experts considère qu'il n'y pas d'obligation en ce sens et que l'État reste libre de choisir la forme de contre-mesures qu'il adopte tant qu'elle respecte conditions liées à la prise de contre-mesures (commentaire sous la règle 20 – §9, p. 119).

La prise de contre-mesures est soumise à plusieurs conditions procédurales importantes prescrites par l'article 52(1) des Articles de la CDI sur la responsabilité de l'État. Ainsi, **avant de prendre des contre-mesures, l'État lésé doit** (commentaire sous la règle 20 – §§ 10-13, pp. 120-121) :

- **demander à l'État responsable de s'acquitter de ses obligations** ;
- **notifier l'État responsable de toute décision de prendre des contre-mesures et offrir de négocier avec cet État.**

L'obligation de notifier est particulièrement à propos pour les cyber opérations puisque leur origine peut avoir été usurpée, pour faire croire qu'elles proviennent d'un État qui n'est pas responsable (commentaire sous l'article 20 – §12, p. 120). Néanmoins, l'article 52(2) des Articles de la CDI sur la responsabilité de l'État prévoit une exception, reprise dans le commentaire du *Manuel de Tallinn* (§ 12, p. 120) : l'État lésé peut prendre des **contre-mesures urgentes**, c'est-à-dire sans notification préalable, qui sont nécessaires pour préserver ses droits. Les spécificités techniques des technologies de l'information rendent particulièrement pertinente et nécessaire la possibilité pour l'État lésé d'avoir recours à des contre-mesures urgentes.

Il est important de noter que les experts du *Manuel de Tallinn* reprennent l'obligation de notifier, et l'exception des contre-mesures urgentes, mais que **seulement une minorité des experts considère qu'il existe une obligation en droit international coutumier de négociation** (§ 13, pp. 120-121). On peut voir ici une des différences entre le *Manuel de Tallinn 2.0* et les Articles de la CDI sur la responsabilité de l'État, puisque ces derniers considèrent qu'une telle obligation existe. Pour la majorité des experts, l'État lésé peut prendre des contre-mesures avant

[24] A l'inverse, dans le cadre de la légitime défense, les experts du *Manuel de Tallinn 2.0* reconnaissent l'existence d'un droit de légitime défense anticipée comme nous le verrons plus en avant dans cette analyse.

même d'offrir de négocier et les contre-mesures sont possibles même pendant les négociations. Ils considèrent en effet qu'une telle obligation permettrait à l'État responsable de « *control the duration and impact of its breach by deciding when and for how long to conduct 'good faith negociations'* » (§ 13, p. 120–121). L'approche et les arguments mis en avant par la majorité des experts sont assez peu convaincants. L'obligation prescrite par la CDI est seulement une obligation d'offrir de négocier. Par conséquent, même si l'on peut douter de la bonne foi de l'État responsable dans la conduite des négociations, cela n'altère en rien la possibilité pour l'État lésé de prendre des contre-mesures. De plus, il convient de souligner que la possibilité pour l'État de prendre des contre-mesures urgentes dans certaines circonstances couvre aussi l'obligation d'offrir de négocier en plus de l'obligation de notifier.

Une autre divergence entre le *Manuel de Tallinn 2.0* et les Articles de la CDI sur la responsabilité de l'État concerne l'obligation de ne pas prendre de contre-mesures ou d'y mettre un terme si *« le différend est en instance devant une cour ou un tribunal habilité à rendre des décisions obligatoires pour les parties »* (article 52(3)(b) des Articles de la CDI sur la responsabilité de l'État). La CDI a reconnu l'existence de cette obligation, alors que seule la majorité, et non l'ensemble, des experts du *Manuel de Tallinn 2.0* considère qu'une telle obligation existe en droit coutumier (commentaire sous la règle 20 – §13, pp. 120-121).

Aux termes de la **règle 22**, **les contre-mesures, de nature cyber ou non, ne peuvent porter atteinte aux obligations concernant la protection des droits fondamentaux de l'homme, constituer des représailles et violer des normes impératives de droit international**. La règle précise dans une seconde phrase que l'État prenant des contre-mesures doit respecter ses obligations liées à l'inviolabilité des locaux, agents archives et documents consulaires et diplomatiques. Les différentes obligations reprises dans la règle ne posent pas de problèmes particuliers dans le domaine numérique et nous allons donc nous concentrer sur une différence importante entre la règle 22 et les Articles de la CDI sur la responsabilité de l'État concernant les contre-mesures armées.

En effet, la première phrase de la règle « [c]*ountermeasures, whether cyber in nature or not, may not include actions that affect fundamental human rights, amount to prohibited belligerent reprisals, or violate a peremptory norm* » reprend l'article 50(1) des Articles de la CDI sur la responsabilité de l'État avec quelques différences. L'article 50(1) des Articles de la CDI sur la responsabilité de l'État précise que :

> « 1. Les contre-mesures ne peuvent porter aucune atteinte :
>
> a) À l'obligation de ne pas recourir à la menace ou à l'emploi de la force telle qu'elle est énoncée dans la Charte des Nations Unies ;
>
> b) Aux obligations concernant la protection des droits fondamentaux de l'homme ;
>
> c) Aux obligations de caractère humanitaire excluant les représailles ;
>
> d) Aux autres obligations découlant de normes impératives du droit international général. »

Il est intéressant de voir que l'alinéa (*a*) de l'article 50(1) n'a pas été repris dans la règle 22, mais que l'interdiction des contre-mesures portant atteinte à l'interdiction du recours à la menace ou à l'emploi de la force est néanmoins discutée dans le commentaire sous les règles 20 (§ 2, pp. 111-112) et 22 §§1, 9-15, pp.123-126). La mention de cette obligation seulement dans le commentaire et non dans le texte des règles peut sembler curieuse et amène à s'interroger sur les raisons d'un tel choix. La justification de ce choix est sûrement à trouver dans le fait qu'une minorité d'experts participant à la rédaction du *Manuel de Tallinn 2.0* considère qu'il existe des formes armées de contre-mesures (commentaire sous la règle 22, § 12, pp. 125-126).

Il existe en effet en droit international un courant minoritaire d'auteurs qui défendent la possibilité pour les États de prendre des **contre-mesures armées**, c'est-à-dire des contre-mesures impliquant le recours à la menace ou l'emploi de la force.

Cette approche a notamment trouvé écho dans l'*Opinion individuelle* du Juge Simma dans l'affaire des *Plates-formes pétrolières* :

> « Pour résumer mes vues sur les questions du recours à la force et de la légitime défense telles qu'elles se posent en l'espèce, il convient de distinguer deux degrés : il y a d'abord le degré des attaques armées massives et de grande ampleur, qui constituent « une agression armée » pour reprendre les termes de l'article 51. Face à une telle agression, la légitime défense, dans ses formes non pas infiniment, mais néanmoins considérablement variées, serait justifiée. Mais il existe aussi des actes militaires hostiles d'un degré inférieur, qui n'atteignent pas le seuil de l'« agression armée » au sens de l'article 51 de la Charte des Nations Unies. Contre les actes hostiles de ce genre, un Etat peut bien entendu se défendre, mais uniquement par des mesures dont la portée et la nature sont plus restreintes (la principale différence résidant dans le fait que la possibilité de légitime défense collective n'existe pas dans ce cas, voir *Nicaragua*), et qui doivent aussi être très rigoureusement nécessaires et proportionnées, et suivre immédiatement l'acte qui les a motivées. »[25]

Il précise par la suite que dans le cas d'espèce, il serait possible de répondre à un recours à la force ne constituant pas une agression armée, et donc n'ouvrant pas la possibilité pour l'État de victime d'invoquer son droit de légitime défense, par « *des 'contre-mesures proportionnées' également de nature militaire* »[26].

Cette approche se base sur l'existence d'un écart entre le seuil du recours à la menace ou à l'emploi de la force de l'article 2(4) de la Charte des Nations Unies, et le seuil de l'agression armée de l'article 51. Dans cet écart, l'Etat pourrait être victime d'actes impliquant la menace ou l'emploi de la force d'une intensité limitée sans avoir la possibilité de répondre par des mesures impliquant la menace ou l'emploi de la force. Cette situation entraîne, aux termes de cette approche, un déséquilibre entre l'État victime et l'État responsable, qui serait corrigé en autorisant l'État victime à adopter des contre-mesures armées proportionnées à l'acte de l'État responsable. Il convient de rappeler ici qu'il s'agit d'un courant de pensée minoritaire dans la doctrine du droit international qui n'a pour le moment pas trouvé écho dans la pratique ou les positions des États.

En lien avec la question des contre-mesures armées, le commentaire rappelle que certains États considèrent que les seuils des articles 2(4) et 51 sont équivalents (§ 15, p. 126). Ainsi, tout emploi de la force équivaudrait à une agression armée ouvrant droit à la légitime défense. Par conséquent, pour ces États le débat sur l'existence des contre-mesures armées est superflu puisqu'ils considèrent que tout emploi de la force leur permet d'invoquer leur droit de légitime défense.

La **règle 23** rappelle que **les contre-mesures doivent être proportionnelles au préjudice subi**. Cette règle reprend la première partie de l'article 51 des Articles de la CDI sur la responsabilité de l'État. La seconde partie précise qu'elles doivent être proportionnelles *« compte tenu de la gravité du fait internationalement illicite et des droits en cause »* (repris dans le commentaire sous la règle 23 – §1, p. 127).

---

25 *Plates-formes pétrolières (République islamique d'Iran c. États-Unis d'Amérique),* (arrêt), 2003, p. 333, § 13.

26 *Ibid.*, p. 333, § 14.

L'évaluation de la proportionnalité est analysée dans le commentaire (§§ 4-5, p. 128) qui reprend en substance une partie du commentaire sous l'article 51 des Articles de la CDI sur la responsabilité de l'État :

> « Comme il faut garantir que l'adoption de contre-mesures n'aboutisse pas à des résultats inéquitables, la proportionnalité doit être évaluée compte tenu non seulement de l'élément purement « quantitatif » du préjudice subi, mais aussi compte tenu de facteurs « qualitatifs » comme l'importance de l'intérêt protégé par la règle violée et la gravité de la violation. L'article 51 lie la proportionnalité en premier lieu au préjudice subi, mais « compte tenu » des deux autres critères : la gravité du fait international illicite et les droits en cause. L'expression « les droits en cause » a un sens large, et vise non seulement les effets d'un fait illicite sur l'État lésé, mais aussi les droits de l'État responsable. En outre, la situation d'autres États susceptibles d'être affectés peut aussi être prise en considération ».[27]

En revanche, l'obligation de proportionnalité n'implique pas une obligation de réciprocité entre l'obligation violée par l'État responsable et la forme choisie de contre-mesures (commentaire sous la règle 23 – §7, pp. 128-129). Ceci implique notamment que des contre-mesures à caractère numérique pourront être adoptées contre un fait internationalement illicite non numérique, et vice versa.

Le groupe d'experts considère qu'il n'existe pas d'obligation pour l'État lésé de prendre des mesures pour atténuer le préjudice subi avant de prendre des contre-mesures. L'absence de prise de mesures visant à atténuer le préjudice subi n'affecte en rien la proportionnalité des contre-mesures concernées (commentaire sous la règle 23 – §9, p. 129).

La **règle 24** précise que **seul l'État lésé peut prendre des contre-mesures**. Il s'agit d'une précision importante avec conséquences principales. D'un côté, les acteurs non étatiques ne peuvent pas prendre de contre-mesures sauf s'ils agissent pour le compte d'un État (commentaire sous la règle 24 – §2, p. 130). En effet, l'État lésé peut décider d'avoir recours à des acteurs non étatiques agissant pour son compte pour prendre des contre-mesures (§ 3, p. 131). D'un autre côté, **seul l'État lésé peut prendre des contre-mesures, c'est-à-dire que les États tiers n'ont pas le droit d'adopter de contre-mesures et qu'il n'y a pas de contre-mesures collectives, à l'inverse de la légitime défense comme l'a rappelé la CIJ dans l'affaire *Nicaragua***[28]. Néanmoins, les experts participant au *Manuel de Tallinn* sont partagés sur ce point (§§ 5-9, pp. 131-132). La majorité des experts reprend l'interdiction des contre-mesures collectives formulées par la CIJ, alors qu'une minorité d'experts considère qu'il est possible pour un État tiers de prendre des contre-mesures à la demande de l'État lésé (§7).

Les experts sont aussi partagés sur la question de l'assistance qu'un État tiers peut apporter à l'État lésé dans la conduite de contre-mesures. Trois vues se distinguent parmi les experts :

- Pour certains, les mesures servant à faciliter la prise de contre-mesures par l'État lésé ne peuvent être distinguées des contre-mesures elles-mêmes et sont donc proscrites.
- Pour d'autres, la licéité de ces mesures dépend de si ces mesures violent une obligation de l'État les prenant envers l'État visé par les contre-mesures. Si ces mesures violent une telle obligation, alors elles seront considérées comme un acte internationalement illicite de l'État qui les adopte à l'encontre de l'État visé.

---

27 « Projet d'articles sur la responsabilité de l'État pour fait internationalement illicite et commentaires y relatifs », *Annuaire de la Commission du droit international*, 2001, II(2), p. 31‑143, commentaire sous l'article 51, para 6, p. 370.

28 *Activités militaires et paramilitaires au Nicaragua et contre celui-ci (Nicaragua c. Etats-Unis d'Amérique)* (fond), 1986, p. 127, para 249.

- Pour le troisième groupe, les mesures d'assistance sont licites, car elles doivent être distinguées des contre-mesures.

La **règle 25** rappelle que **les contre-mesures, de nature numérique ou non, qui violent les obligations de l'État envers des États tiers ou d'autres parties sont interdites**. En d'autres termes, l'illicéité des actes pris comme contre-mesures par l'État lésé ne sera exclue que par rapport à l'État responsable, les actes affectant d'autres États seront considérés comme des faits internationalement illicites de l'État qui les adoptent envers les États concernés.

L'utilisation de l'expression « autres parties » fait référence aux entités non étatiques envers lesquelles l'État pourrait posséder des obligations en vertu du droit international, notamment des organisations internationales voire des individus (commentaire sous la règle 25 – §2, p. 133).

3.2.4.3 État de nécessité (Chapitre 4, section 2 [*suite*] – règle 26)

Aux côtés de la légitime défense et des contre-mesures, une dernière circonstance excluant l'illicéité à fait l'objet d'une règle distincte : l'état de nécessité[29]. Aux termes de la **règle 26**, qui reprend en substance et adapte l'article 25(1)(a) des Articles de la CDI sur la responsabilité de l'État[30], **un État peut invoquer l'état de nécessité en réponse à un acte qui constitue un péril grave et imminent, de nature numérique ou non, pour un intérêt essentiel lorsqu'agir ainsi et le seul moyen de le protéger**. Ainsi, l'État de nécessité permet d'exclure l'illicéité d'actes qui constituent le seul moyen pour l'État de protéger un intérêt essentiel contre un péril grave et imminent.

Le groupe d'experts reconnaît la dimension coutumière de ce principe (commentaire sous la règle 26 – §1, p. 135). Il souligne par ailleurs que la notion *« d'intérêt essentiel »* n'est pas clairement définie, mais qu'elle diffère néanmoins de celle d'organismes d'importance vitale (§ 2, pp. 135-136). Cependant, la plupart des cyber opérations visant des organismes d'importance vitale pourraient certainement être considérées comme visant un intérêt essentiel de l'Etat (voir notamment les exemples fournis par le groupe d'experts – §5, pp. 136-137), encore faudrait-il que le péril qui en découle soit à la fois grave et imminent pour permettre à l'État d'invoquer l'état de nécessité (§ 4, p. 136).

L'État peut invoquer l'état de nécessité pour exclure l'illicéité d'actes qu'il prendrait et qui affecteraient les droits d'État non responsable de la situation (commentaire sous la règle 26 – §6, p. 137). En effet, l'état de nécessité ne dépend pas de l'existence d'un fait internationalement illicite antérieur (§ 9, p. 137). Par conséquent, il n'implique pas qu'il y ait nécessairement une attribution de l'acte à un État, et notamment à l'État concerné par les mesures prises pour lesquelles l'État auteur invoque l'état de nécessité (§ 10, p. 138).

L'état de nécessité ne peut être invoqué que si le péril est imminent, le groupe d'experts estime que le péril n'a pas besoin de s'être réalisé, mais que la « fenêtre d'opportunité » *(window of opportunity)* doit être sur le point de prendre fin. Ainsi, l'État pourrait prendre des mesures préventives en invoquant l'état de nécessité (commentaire sous la règle 26 – §15, p. 139).

---

29 Christian Schaller, dans un article préparé dans le cadre du *Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* analyse l'approche du Manuel de Tallinn 2.0 sur l'état de nécessité. Il critique notamment l'approche choisie, en soulignant que l'analyse du Manuel de Tallinn 2.0 semble aller au-delà de la *lex lata* et adopte certaines approches qui ne font pas consensus. Il souligne le risque de d'abus si on adopte une interprétation trop large de l'état de nécessité dans le domaine numérique. SCHALLER C., « Beyond Self-Defense and Countermeasures: A Critical Assessment of the *Tallinn Manual*'s Conception of Necessity [*Symposium:* Tallinn Manual 2.0 *on the International Law Applicable to Cyber Operations*] », *Texas Law Review*, 2017 2016, vol. 95, p. 1619‑1638.

30 Voir la comparaison entre la règle 26 du Manuel de Tallinn 2.0 et l'article 25(1)(a) des Articles de la CDI sur la responsabilité de l'État faite par Christian Schaller : *Ibid.*, p. 1613‑1614.

L'article 25 des Articles de la CDI sur la responsabilité de l'État fixe certaines limites reprises dans le commentaire. Ainsi, les actes ne doivent pas porter gravement atteinte à un intérêt essentiel des États concernés (commentaire sous la règle 26 – §8, p. 137) et l'Etat ne doit pas avoir contribué à la survenance de la situation (§ 19, p. 140)

Le groupe d'experts est divisé sur la question de savoir si l'état de nécessité peut être invoqué pour justifier des mesures impliquant le recours à la force (commentaire sous la règle 26 – §18, p. 140). Certains experts considèrent qu'il ne s'agit pas d'une exception valable à l'interdiction générale du recours à la force (droit coutumier et article 2, paragraphe 4, de la Charte des Nations Unies) alors que d'autres estiment que dans certains cas seules des mesures impliquant le recours à la force pourraient protéger l'intérêt essentiel menacé et seraient donc justifiées par l'état de nécessité. Cette discussion et les arguments avancés pour justifier la possibilité de recourir à des mesures impliquant le recours à la force sont peu convaincants. **Ces arguments semblent faire échos à ceux mis en avant pour justifier l'existence de contre-mesures armées. Il nous semble important de rappeler qu'il n'existe en droit international qu'un nombre très limité d'exceptions à l'interdiction du recours à la force, tant dans la Charte des Nations Unies qu'en droit coutumier, et l'état de nécessité n'en fait pas partie.**

3.2.4.4 Obligations des États relatives à un fait internationalement illicite (Chapitre 4, section 3 – règles 27 à 30)

La troisième section, du quatrième chapitre, du *Manuel de Tallinn 2.0* s'intéresse aux obligations des États relatives aux faits internationalement illicites et comporte quatre règles qui sont pour une grande partie inspirées des de la seconde partie « Contenu de la responsabilité internationale de l'État » (articles 28 à 41) des Articles de la CDI sur la responsabilité de l'État.

L'État responsable d'un fait internationalement illicite mené par des moyens numériques a l'obligation d'y mettre fin et, si les circonstances l'exigent, d'offrir des assurances et garanties de non-répétition (**règle 27**). Cette règle paraphrase l'article 30 des Articles de la CDI sur la responsabilité de l'État.

L'État lésé, ou les États lésés lorsqu'ils sont plusieurs, par un fait internationalement illicite sont en droit d'invoquer la responsabilité de l'État responsable qui a violé une obligation qui leur est due (article 42 des Articles de la CDI sur la responsabilité de l'État) et donc à lui demander la cessation du fait illicite, ainsi que des assurances et garanties de non-répétition (commentaire sous la règle 27 – §1, p. 142).

Le commentaire sous la règle 27 reprend l'analyse des **assurances et garanties de non-répétition** du commentaire sous l'article 30 des Articles de la CDI sur la responsabilité de l'État. Il convient ainsi de souligner que *« [l]es assurances et garanties visent à rétablir la confiance dans une relation continue, bien qu'elles offrent beaucoup plus de souplesse que la cessation et ne soient pas exigées dans tous les cas »*[31]. Il s'agit de deux notions différentes, d'un côté, les '*assurances*' sont normalement données oralement ou sous forme de communications, de l'autre côté, les '*garanties de non-répétition*' impliquent la prise de mesures visant à assurer la non-répétition du fait internationalement illicite (commentaire sous la règle 27 – §5, p. 143 ; voir aussi commentaire sous l'article 30 des Articles de la CDI sur la responsabilité de l'État – § 12, p. 238). Les assurances et garanties de non-répétition ne sont pas automatiques, mais dépendent des circonstances et du fait internationalement illicite concerné (commentaire sous la règle 27 – §§6-7, p. 143). Les experts soulignent que dans leurs commentaires sur les Articles de la CDI sur la responsabilité de l'État, les États-Unis ont indiqué que les assurances et garanties de non-répétition ne constituaient pas une obligation juridique, mais plutôt une pratique diplomatique (commentaire sous la règle 27 – §8, p. 144).

31 « Articles de la CDI sur la responsabilité de l'État », *op. cit.* commentaire sous l'article 30, para 9, p. 236.

Les règles 28 et 29 s'intéressent à la réparation du préjudice subi. Ainsi, **l'État responsable est tenu de réparer intégralement le préjudice causé par le fait internationalement illicite mené par des moyens numériques** (**règle 28**). Cette règle reprend l'article 31(1) des Articles de la CDI sur la responsabilité de l'État. La **règle 29** concerne les formes de réparation, et précise que **la réparation du préjudice causé par un fait internationalement illicite mené par des moyens numériques prend la forme de restitution, d'indemnisation et de satisfaction**. Cette règle reprend la première partie de l'article 34 des Articles de la CDI sur la responsabilité de l'État.

L'objectif de la réparation du préjudice causé par un acte internationalement illicite a été précisé par la CIJ dans l'affaire de l'*Usine de Chorzów* :

> « Le principe essentiel, qui découle de la notion même d'acte illicite et qui semble se dégager de la pratique internationale, notamment de la jurisprudence des tribunaux arbitraux, est que la réparation doit, autant que possible, effacer toutes les conséquences de l'acte illicite et rétablir l'état qui aurait vraisemblablement existé si ledit acte n'avait pas été commis. »[32].

Le préjudice, sur lequel repose l'obligation de réparation, *« **comprend tout dommage, tant matériel que moral, résultant du fait internationalement illicite de l'État** »* (commentaire sous la règle 28 – §2, p.144). **L'obligation de réparation ne concerne que le préjudice causé par l'acte internationalement illicite** (commentaire sous la règle 28 – §§6-7, pp. 145-146), et non toutes les conséquences de ce fait[33].

L'État lésé n'a pas d'obligation de prendre des mesures pour atténuer le préjudice subi. Néanmoins, il pourra être pris en compte dans l'évaluation de la réparation appropriée le fait que l'État lésé pouvait prendre de telles mesures, mais ne l'a pas fait. L'État lésé ne pourra donc prétendre obtenir réparation pour les dommages qu'il aurait raisonnablement pu éviter (commentaire sous la règle 28 – §8, p. 146). De la même manière, *« la contribution au préjudice due à l'action ou l'omission, intentionnelle ou par négligence, de l'Etat lésé est prise en compte dans la détermination de la réparation »*[34] (commentaire sous la règle 28 – §9, p. 147).

En cas de pluralité d'États responsables pour un même fait internationalement illicite, la responsabilité de chaque État peut être invoquée par rapport à ce fait et il peut lui être demandé de réparer l'intégralité du préjudice causé, dans la limite où l'État lésé ne peut pas recevoir une indemnisation supérieure au dommage qu'il a subi (commentaire sous la règle 28 – §11, p. 147). Il s'agit ici de l'article 47 des Articles de la CDI sur la responsabilité de l'État. **Il convient de distinguer le cas où les Etats mènent conjointement un même fait internationalement illicite, du cas où plusieurs faits internationalement illicites menés par différents Etats contribuent à un même préjudice**. Dans ce second cas de figure, **chaque État ne sera responsable que du fait internationalement illicite qu'il a mené et du préjudice qui en résulte**, et non du préjudice global résultant de la somme des faits internationalement illicites des différents États contributeurs (§§ 12-13, p148).

La règle 29 détaille les trois formes de réparation : restitution, indemnisation et satisfaction. Ces différentes formes de réparations peuvent être mises en œuvre séparément ou conjointement, selon les circonstances (commentaire sous la règle 29 – §1, pp. 148-149).

---

32 *Usine de Chorzów* (fond), 1928, p. 27.

33 « Articles de la CDI sur la responsabilité de l'État », *op. cit.*, commentaire sous l'article 31, paras 9-10, pp. 244-245.

34 Article 39, Articles de la CDI sur la responsabilité de l'État.

La forme première et principale de réparation est la restitution[35], c'est-à-dire le rétablissement de la situation qui existait avant que le fait illicite ne soit commis (commentaire sous la règle 29 – §§2-5, pp.149-150).

Lorsque le dommage causé n'est pas réparé par la restitution, l'Etat responsable du fait internationalement illicite est tenu d'**indemniser**[36] le dommage causé par ce fait. L'indemnisation à une acception large, elle couvre non seulement les pertes financières et les dommages subis par l'État, mais peut aussi couvrir ceux subis par des acteurs non étatiques, notamment des entreprises privées (commentaire sous la règle 29 – §7, p. 150). Comme le souligne le commentaire sous l'article 36 de la CDI, on parle ici de dommage et non de préjudice, car l'indemnisation ne concerne que les dommages matériels et moraux (article 36 des Articles de la CDI sur la responsabilité de l'État), mais pas d'éventuels préjudices moraux causés à l'État lésé qui seront réparés par la satisfaction.

Lorsque le préjudice causé n'est pas réparé ni par la restitution ni par l'indemnisation, l'État du fait internationalement illicite est tenu de donner **satisfaction**[37]. Comme le précise l'article 37(2) de la CDI, repris dans le commentaire du *Manuel de Tallinn 2.0*, *« La satisfaction peut consister en une reconnaissance de la violation, une expression de regrets, des excuses formelles ou toute autre modalité appropriée »* (commentaire sous la règle 29 – §§9-11, pp. 151-152).

Finalement, la dernière règle de cette section dédiée aux obligations des États relatives aux faits internationalement illicites concerne la violation d'une obligation due à la communauté internationale dans son ensemble (**règle 30**) : **tout État peut invoquer la responsabilité de l'État qui a mené des cyber opérations violant une obligation *erga omnes* due à la communauté internationale dans son ensemble**. Cette règle reprend l'article 48(1)(b) des Articles de la CDI sur la responsabilité de l'État.

3.2.4.5 Responsabilité des organisations internationales (Chapitre 4, section 5 – règle 31)

Les organisations internationales sont responsables aux termes du droit international pour leurs actes ou omissions à dimension numérique qui constituent des faits internationalement illicite (commentaire introductif à la section 5 du chapitre 4 – §1, p. 153). La règle et le commentaire subséquents du *Manuel de Tallinn 2.0* sur la responsabilité des organisations internationales sont pour une grande partie basés sur le Projet d'Articles sur la responsabilité des organisations internationales de la CDI[38] qui reflète le droit international coutumier en la matière (§ 1, p. 154).

Le commentaire introductif de la section sur la responsabilité des organisations internationales souligne que :

> « [w]hile some international organisations rely heavily on the cyber infrastructure of Member States and have limited capacity of their own, others own and operate significant cyber infrastructure. Furthermore, while some international organisations are limited to cyber defence, other may be in position to conduct offensive cyber operations, using either assets of Member States or those owned or controlled by the organisation itself » (§7, p. 155)

Cette assertion peut paraître curieuse puisqu'à notre connaissance, aucune organisation internationale ne s'est vu accorder le droit par ses États membres de mener des cyber opérations

35 Article 35, Articles de la CDI sur la responsabilité de l'État.

36 Article 36, Articles de la CDI sur la responsabilité de l'État.

37 Article 37, Articles de la CDI sur la responsabilité de l'État.

38 Commission du droit international de l'ONU, Projet d'Articles sur la responsabilité des organisations internationales, document des Nations Unies A/66/10, *Annuaire de la Commission du droit international, 2011,* vol. II(2).

offensives. Le développement des capacités numériques et la conduite d'activités numériques par ces organisations internationales n'ont en effet pour but que d'assurer la protection de leurs systèmes d'information. Elle semble donc plus concerner une éventuelle évolution future du rôle et des compétences en matière numérique des organisations internationales que la situation actuelle.

Le commentaire introductif souligne par ailleurs qu'à l'inverse des États, **les organisations internationales n'exercent pas de souveraineté** et ne peuvent donc pas invoquer la violation de leur souveraineté pour justifier la prise de mesures unilatérales (§9, pp.155-156). À l'inverse, **les experts considèrent que les organisations internationales sont tenues par l'obligation de non-intervention et celle de ne pas violer la souveraineté des États** (§10, p.156).

Une précision importante : le groupe d'expert considère, à juste titre, que l'interdiction du recours à la menace ou à l'emploi de la force de l'article 2(4) de la Charte des Nations Unies ne s'applique pas aux organisations internationales, mais seulement aux États membres de l'Organisation des Nations Unies (§ 12, p. 156). Le commentaire note que les experts *« refrained from taking a position as to whether the customary law prohibition of the threat or use of force binds international organisations with respect to their cyber operations. However, the Experts drew attention to the general rule that a State incurs international responsibility if it causes an international organisation of which it is a Member to commit an act that, if committed by that State, would constitute a breach of an international obligation binding it »* (§ 12, p.157).

Le *Manuel de Tallinn 2.0* ne comporte qu'une seule règle sur la responsabilité des organisations internationales, aux termes de laquelle **une organisation internationale est responsable en droit international pour toute cyber opération qui viole une obligation internationale et qui est attribuable à cette organisation** (**règle 31**). Cette règle reprend l'article 4 du Projet d'Articles de la CDI sur la responsabilité des organisations internationales. On peut s'interroger sur ce choix, qui résulte en une règle générale et un commentaire très long touchant à des questions aussi diverses que variées, plutôt que d'adopter plusieurs règles sur les différentes questions relatives à la responsabilité des organisations internationales. Le commentaire du *Manuel de Tallinn 2.0* n'explique pas ce choix.

La cyber opération concernée doit être **attribuable à l'organisation internationale** pour qu'elle soit responsable. Les comportements des organes et des agents d'une organisation internationale dans l'exercice de leurs fonctions lui sont attribuables[39] (commentaire sous règle 31 – §§2-4, pp. 157-158), s'ils ont agi en leur qualité officielle et dans le cadre des fonctions générales de l'organisation, même s'ils outrepassent sa compétence ou contreviennent à ses instructions[40] (§§ 6-7, p. 159). Il en va de même pour les organes ou agents d'un État ou d'une autre organisation internationale mis à la disposition de l'organisation internationale (§§ 8-10, pp. 159-160).

Une organisation internationale peut aussi être responsable du fait internationalement illicite d'un État ou d'une autre organisation internationale si elle apporte son aide ou son assistance dans la commission de ce fait, si elle donne des directives et contrôle sa commission ou si elle exerce une contrainte sur l'État ou l'organisation internationale qui commet ce fait (§§ 11-17, pp.161-163). Il s'agit ici de la reprise des dispositions des articles 14, 15 et 16 du Projet d'Articles de la CDI sur la responsabilité des organisations internationales.

De la même manière, l'organisation internationale ne peut pas contourner ses obligations internationales en adoptant une décision imposant à des États ou des organisations internationales membres de commettre un fait qui serait internationalement illicite s'il avait été

39 Article 6, Projet d'Articles de la CDI sur la responsabilité des organisations internationales.

40 Article 8, Projet d'Articles de la CDI sur la responsabilité des organisations internationales.

commis par elle (§§ 18-19, pp. 163-164). Il s'agit ici de l'article 17(1) du Projet d'Articles de la CDI sur la responsabilité des organisations internationales. Il est intéressant de noter que l'article 17(2) étend la responsabilité de l'organisation internationale pour le fait d'autoriser, et non seulement d'imposer, à des États ou des organisations internationales membres de commettre un fait qui serait internationalement illicite s'il avait été commis par elle. À l'inverse de la CDI, les experts du *Manuel de Tallinn 2.0* considèrent qu'il n'est pas possible d'identifier une telle obligation en droit international coutumier et notent leur désaccord par rapport au Projet d'Articles de la CDI sur la responsabilité des organisations internationales (§ 22, p. 165).

Finalement, le commentaire sous la règle 31 s'intéresse à la question des **circonstances excluant l'illicéité** (§§ 23-27, pp. 165-167). Le Projet d'Articles de la CDI sur la responsabilité des organisations internationales identifie six circonstances excluant l'illicéité : le consentement (article 20), la légitime défense (article 21), les contre-mesures (article 22), la force majeure (article 23), la détresse (article 24) et l'état de nécessité (article 25). La majorité des experts est d'accord pour considérer que dans certaines circonstances l'illicéité des actes d'une organisation internationale peut être exclue, mais les experts ne sont pas d'accord sur la question de savoir quelles circonstances sont applicables dans le cas des actes commis par une organisation internationale. Seule une minorité d'experts considère comme applicables les six circonstances identifiées par la CDI. Par exemple, les experts sont partagés quant à la question de savoir si une organisation internationale peut adopter des contre-mesures pour contraindre un État ou une organisation internationale, membres ou tiers, à mettre un terme à la violation d'une obligation internationale due à cette organisation internationale. (§ 27, p. 166).

3.2.5 Les cyber opérations qui ne sont pas *per se* encadrées par le droit international (chapitre 5 – règles 32 et 33)

Le titre du cinquième chapitre « *Cyber operations not* per se *regulated by international law* », que l'on peut traduire par « Les cyber opérations qui ne sont pas par elles-mêmes encadrées par le droit international », soulève quelques questions. Premièrement, il sous-entend que certains types de cyber opérations seraient encadrées par le droit international et pas d'autres, posant ainsi la question de ce qui différencie ces cyber opérations des autres. Le cinquième chapitre contient deux règles traitant respectivement de l'espionnage numérique en temps de paix (règle 32) et des cyber opérations conduites par des acteurs non étatiques (règle 33). La formulation du titre sous-entendrait donc que les cyber opérations sont en général encadrées par le droit international en tant que cyber opérations, sauf si elles constituent des actes d'espionnage en temps de paix ou sont conduites par des acteurs non étatiques.

La formulation utilisée pour le titre de ce chapitre nous semble trompeuse et suggère une certaine vision du droit international qui nous paraît discutable, une vision qui va à l'encontre de l'approche traditionnelle, surtout en ce qui concerne l'espionnage et le régime juridique des cyber opérations en général. Nous traiterons séparément la question de l'espionnage et celle des cyber opérations conduites par des acteurs non étatiques.

3.2.5.1 Cyber espionnage en temps de paix

Avant d'analyser le statut des actes de cyber espionnage en droit international, il convient de rappeler celui de l'espionnage et des cyber opérations.

3.2.5.1.1 Licéité de l'espionnage

En droit international, rien n'interdit aux États de mener des activités d'espionnage, ce que rappelle le groupe d'experts (commentaire sous la règle 32 – §5, p. 169). En d'autres termes, l'espionnage en temps de paix ne constitue pas en lui-même un acte internationalement illicite. Cette analyse de la licéité de l'espionnage fait consensus. **Néanmoins, deux courants de pensée s'affrontent sur la licéité des actes d'espionnage.**

Le courant majoritaire considère que l'espionnage n'est pas illicite en lui-même et qu'aucune norme de droit international ne limite la possibilité pour les États de mener des activités d'espionnage, mais que ces activités peuvent constituer des violations du droit international si elles violent de normes spécifiques du droit international. À titre d'exemple, il tout à fait licite pour un État d'espionner un autre État, mais le fait d'envoyer ses agents sur le territoire d'un autre État constituerait une violation de la souveraineté de cet État. Cette approche est celle adoptée par les experts du Manuel de Tallinn 2.0 (règle 32 et commentaire sous la règle 32 – §6, p. 170).

Le courant minoritaire adopte une approche que l'on peut qualifier de fonctionnelle. Il considère que l'espionnage n'est pas illicite en droit international et que cela rejaillit sur les actes d'espionnage. Ainsi, ces actes qui devraient constituer des actes internationalement illicites en temps normal, comme la violation de la souveraineté d'un État, ne seraient pas illicites, car perpétrés à des fins d'espionnage et que l'espionnage est licite en droit international.

3.2.5.1.2 Licéité des cyber opérations

La licéité des cyber opérations est similaire à celle de l'espionnage. Rien n'interdit en droit international aux États de mener des cyber opérations, ce n'est pas illicite *per se*, mais il convient d'analyser la licéité de chaque cyber opération au cas par cas. Ainsi, il est licite pour un Etat de conduire des cyber opérations, mais ces cyber opérations peuvent constituer des actes

internationalement illicites si elles violent des normes de droit international, notamment la souveraineté d'un autre État, le principe de non-intervention ou encore l'interdiction du recours à la force.

Il est donc curieux de voir le titre de ce chapitre sous-entendre que certaines cyber opérations seraient encadrées par le droit international et pas d'autres. Nous allons y revenir.

3.2.5.1.3 Cyber espionnage

Le *Manuel de Tallinn 2.0* suit la vision traditionnelle selon laquelle le cyber espionnage n'est pas illicite en soit, mais que les actes d'espionnage numérique peuvent constituer des actes internationalement illicites dans certains cas. La formulation de la **règle 32** est explicite en ce sens : **bien que le cyber espionnage en temps de paix ne constitue pas en lui-même une violation du droit international, les moyens mis en œuvre peuvent constituer des violations du droit international**, et le commentaire des experts reprécise leur approche (règle 32 et commentaire sous la règle 32 – §6, p. 170 ; voir aussi commentaire sous la règle 4 – §27, p. 25).

Cepednant le titre du chapitre, ainsi que la longueur du commentaire sous la règle 32, laissent entrevoir une certaine sympathie pour l'approche fonctionnelle et pourraient avoir pour conséquence d'induire le lecteur en erreur. En effet, ces éléments pourraient amener le lecteur à penser que parce qu'une cyber opération serait conduite à des fins d'espionnage elle ne serait pas encadrée par le droit international de la même manière que si elle avait une autre finalité, même si cela est explicitement rejeté dans le commentaire (§ 12, p. 172).

De plus, le contenu de certains débats qui ont animé le groupe d'experts et qui sont retranscrits dans le commentaire peuvent sembler déroutant. Ainsi, les experts se sont interrogés sur la licéité d'une cyber opération à des fins d'espionnage consistant dans l'insertion d'une clef USB dans l'ordinateur d'un État par une personne agissant sous la direction ou le contrôle d'un autre État (commentaire sous la règle 32 – §§9-10, p. 171-172). La majorité des experts considérant que cela constituerait une violation de la souveraineté de l'État visé, non pas à cause de la dimension numérique de l'action, mais simplement par le fait qu'un individu agissant pour le compte d'un Etat agit sur le territoire d'un autre État sans son accord. Une minorité d'experts considérant de leur côté que cette action ne serait pas illicite, car le fait que l'acte soit conduit à des fins d'espionnage constitue une exception à l'interdiction de la violation de la souveraineté et du principe de non-intervention.

On voit donc ici l'expression des deux courants sur l'espionnage mentionnés précédemment. Néanmoins, on notera une certaine divergence, voire une incohérence entre la règle 32 et le neuvième paragraphe du commentaire sous cette règle. En effet, les règles du *Manuel de Tallinn* sont adoptées par voie de consensus entre les experts. Par conséquent, il semble quelque peu étrange que la règle affirme clairement que l'espionnage n'est pas illicite en soit, mais que les actes d'espionnage peuvent constituer des faits internationalement illicites, alors que dans le commentaire de la règle est mentionnée une vision minoritaire parmi les experts selon laquelle la finalité d'espionnage pourrait constituer une exception qui exclurait illicéité des comportements concernés.

Il aurait peut-être été plus judicieux de simplement rappeler que la conduite de cyber opérations, quel que soit leur finalité, n'est pas illicite en droit international, mais que ces cyber opérations peuvent constituer des actes internationalement illicites.

Pour des questions pratiques, notamment parce que l'espionnage numérique est aujourd'hui une des formes principales de cyber opérations étatiques, il semble justifier d'avoir une règle spécifique sur le sujet, et la formulation de la règle 32 est tout à fait pertinente et claire. Il aurait alors peut-être été plus judicieux de placer cette règle au début en créant un court chapitre

généraliste rappelant que les cyber opérations ne sont pas illicites par elles-mêmes et ce quel que soit leur finalité, mais qu'elles peuvent néanmoins violer certaines normes de droit international, ce qui est d'ailleurs l'objet de plusieurs chapitres du *Manuel de Tallinn 2.0*.

Le groupe d'experts pointe dans son commentaire les spécificités de l'espionnage conduit par des moyens numériques, qui se distingue de l'espionnage classique notamment par sa vitesse et le volume des données concernées (commentaire sous la règle 32 – §4, p. 168). Ils se sont alors interrogés de savoir si ces évolutions avaient aussi entraîné une évolution du droit coutumier applicable en la matière, et ont répondu par la négative (commentaire sous la règle 32 – §5, p. 169). En effet, pour le moment rien ne semble indiquer une volonté des Etats (*opinio juris*) ni une pratique constante permettant d'identifier une évolution du droit international.

Certains experts ont considéré qu'une cyber opération licite pouvait devenir illicite si elle constituait une composante d'une opération illicite alors qu'une minorité d'experts a au contraire affirmé qu'il fallait regarder la licéité de chaque action séparément (commentaire sous la règle 32 – §10, p. 171-172). C'est ici une question complexe qui mérite que l'on s'y attarde. D'un côté, la vision de la majorité des experts semble être la plus en phase avec le droit international et la pratique. Néanmoins, il convient de souligner qu'il n'est pas toujours aisé, et même parfois impossible, de déterminer à quoi vont servir les données collectées et donc d'évaluer la licéité de l'opération finale (commentaire sous la règle 32 – §11 et §13, p. 172-173).

Finalement, les experts se sont intéressés à l'utilisation d'*honeypots* (commentaire sous la règle 32 – §§15-16, p. 173-174). Un *honeypot* est une méthode de cyber défense active consistant à attirer les auteurs de cyber opérations vers des ressources données, souvent sans intérêt, afin de les identifier voire de les neutraliser. Le groupe d'experts distingue trois situations. Premièrement, le fait d'installer un *honeypot* pour surveiller les cyber opérations. Cette situation ne pose pas de difficulté et ne constituerait pas une violation du droit international. Deuxièmement, dans certains cas, le *honeypot* pourrait contenir un fichier compromis contenant un code informatique qui permettrait d'espionner les personnes qui le téléchargeraient. Ainsi, ce code permettrait aux possesseurs du *honeypot* d'espionner les ordinateurs où il aurait été téléchargé et se serait activé. Troisièmement, le fichier mis à disposition pourrait contenir un code malveillant visant à produire des dommages significatifs sur l'ordinateur sur lequel il serait téléchargé et activé.

Dans le second cas, les experts ont conclu qu'il n'y aurait alors pas de violation du droit international puisqu'il s'agirait d'une simple opération d'espionnage qui ne constituerait pas non plus une violation de la souveraineté de l'État si l'État responsable l'avait lui-même transmis dans les systèmes de l'État visé. Cette conclusion semble un peu étrange, puisque la pénétration dans le système de l'État visé constituerait une violation de la souveraineté de cet État, indépendamment qu'il s'agisse d'une cyber opération d'espionnage ou menée à d'autres fins.

Dans le troisième cas, les experts considéraient que le problème résidait dans la question de l'attribution. En d'autres termes, est-ce que les dommages résultant de cette cyber opération sont attribuables à l'État ? Une minorité d'experts a répondu par l'affirmative et considérait qu'il s'agirait d'une violation du droit international, *a minima* une violation de la souveraineté, car l'État responsable avait créé ce dispositif à fins de produire ces dommages. Ils considéraient ainsi que la nature destructrice de l'opération permettait de la qualifier comme une violation du droit international. La majorité des experts considérait à l'inverse que c'est l'organe de l'État victime qui a téléchargé et donc transmis la charge destructrice et que donc l'opération n'est pas attribuable à l'État qui a créé et mis en place le honeypot et le fichier piégé.

3.2.5.2 Cyber opérations conduites par des acteurs non étatiques

La **règle 33** précise que **le droit international n'encadre les cyber opérations conduites par des acteurs non étatiques que dans un nombre limité de cas**.

En effet, les sujets du droit international sont principalement les États et les organisations internationales, alors que les individus et groupes d'individus ne sont généralement pas considérés comme des sujets du droit international. Le droit international est avant tout, et dans une très large majorité, un droit interétatique dont les dispositions ne concernent que les États. Il convient de distinguer les cyber opérations conduites par des acteurs non étatiques selon qu'elles sont ou non attribuables à un État, la règle 33 s'intéressant au second cas de figure. Il convient en effet de rappeler que rien n'interdit à un État d'avoir recours à des acteurs non étatiques pour conduire des cyber opérations, qui lui seront alors attribuables sous certaines conditions, même dans le cadre de la mise en œuvre de contre-mesures (commentaire sous la règle 33 – §4, p. 175).

La règle 33 rappelle que les cyber opérations conduites par des acteurs non étatiques et qui ne sont pas attribuables à un État ne peuvent pas constituer des faits internationalement illicites (commentaire sous la règle 33 – §2, p. 175). Les experts prirent acte, néanmoins, que certains considèrent que des actes d'acteurs privés peuvent être considérés comme violant la souveraineté d'un État.

Par conséquent, les États ne peuvent mener de contre-mesures contre des acteurs non étatiques à l'étranger, mais ils peuvent néanmoins invoquer la responsabilité de l'État d'où agissent ces acteurs pour manquement à son obligation de diligence.

Les experts soulignent deux cas où les États peuvent agir directement contre des acteurs non étatiques : en cas de nécessité en dans le cadre de l'exercice du droit de légitime défense (commentaire sous la règle 33 – §3, p. 175). Le commentaire sous la règle 33 ne donne pas plus de détail sur la légitime défense et, par conséquent, cette conclusion semble un peu rapide. Certains considèrent en effet que l'article 51 de la Charte des Nations Unies ne précise pas que la légitime défense ne peut être invoquée que contre des États, et que donc elle pourrait être utilisée contre des acteurs non étatiques. De plus, un certain nombre d'États ont exercé ces dernières années leur droit de légitime défense contre des acteurs non étatiques. Il s'agit d'un point qui reste controversé en droit international et qui aurait mérité un traitement plus nuancé. Il convient néanmoins de souligner que cette controverse est mentionnée dans le commentaire sous la règle 71 relative à la légitime défense, et que le groupe d'experts étaient partagé sur ce point. La majorité des experts considèrent que la pratique internationale permet d'affirmer l'existence d'un droit de légitime défense contre les actes d'acteurs non étatiques qui atteindrait le seuil de l'agression armée (commentaire sous la règle 71 – §§18-20, pp. 345-346).

Il ne s'agit néanmoins pas d'une observation absolue et le droit international tend de plus en plus à encadrer les activités et comportements des acteurs non étatiques. Dans le cadre d'un conflit armé international ou non international, les acteurs étatiques comme les acteurs non étatiques sont soumis aux règles du droit des conflits armés (commentaire sous la règle 33 – §6, p. 175-176). De la même manière, les acteurs non étatiques conduisant des cyber opérations violant le droit international des droits de l'homme ou le droit pénal international pourraient voir leur responsabilité pénale individuelle engagée dans certaines circonstances aux termes du droit pénal international (commentaire sous la règle 33 – §7, p. 176).

3.3 Certains régimes spécifiques de droit international (Part II. Specialised regimes of international law and cyberspace – pp. 177 à 300 – règles 34 à 64)

La seconde partie du *Manuel de Tallinn 2.0* s'intéresse aux cyber opérations soumises à des normes découlant d'un ou plusieurs régimes spécifiques du droit international.

3.3.1 Droit international des droits de l'homme (chapitre 6 – règles 34 à 38)[41]

Le droit international des droits de l'homme est applicable aux activités ayant une dimension numérique (**règle 34**). De la même manière, **les droits de l'homme dont bénéficient les individus pour leurs activités hors lignes sont aussi applicables à leurs activités en ligne** (**règle 35**).

Le droit international des droits de l'homme est régulièrement confronté à la question de son application extraterritoriale, cette question se pose de manière encore plus marquée en ce qui concerne les activités numériques. Certains considèrent que l'État n'est pas contraint par les droits de l'homme pour les activités se déroulant hors de ces frontières, mais le groupe d'experts est en désaccord avec cette approche et reconnaît l'applicabilité extraterritoriale des droits de l'homme lorsque l'État exerce 'son pouvoir ou son contrôle effectif' (commentaire sous la règle 34 – §7, p. 184). Les experts étaient partagés sur la question de savoir si le pouvoir ou le contrôle effectif d'un État devait s'exercer par des moyens physiques ou pouvait aussi s'exercer par des moyens exclusivement numériques (commentaire sous la règle 34 – §8, p. 185). La majorité est de l'avis qu'il faut un exercice physique du pouvoir ou du contrôle effectif sur un territoire ou un individu (commentaire sous la règle 34 – §9, p. 185).

Les experts ont analysé et discuté une série de droits de l'homme ayant valeur coutumière et qui leur paraissent particulièrement pertinents dans le contexte numérique : le droit à la liberté

---

41 Robert E. Barnsby et Shane R. Reeves, dans un article préparé dans le cadre du *Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,* analysent le traitement des droits de l'homme dans le *Manuel de Tallinn 2.0*. Ils soulignent notamment un certain nombre de points qui peuvent faire débat dans l'approche du *Manuel de Tallinn 2.0* et le fait que le commentaire du *Manuel de Tallinn 2.0* laisse une marge importante d'appréciation aux Etats. REEVES S.R. et R.E. BARNSBY, « Give Them an Inch, They'll Take a Terabyte: How States May Interpret *Tallinn Manual 2.0*'s International Human Rights Law Chapter [*Symposium:* Tallinn Manual 2.0 *on the International Law Applicable to Cyber Operations*] », *Texas Law Review*, 2017 2016, vol. 95, p. 1515‑1530.

L'article de Dinah PoKempner préparé dans le cadre du même symposium offre le point de vue d'une praticienne, elle est *general counsel* chez Human Rights Watch, au regard du traitement des droits de l'homme dans le *Manuel de Tallinn 2.0*. Elle souligne notamment que le groupe d'experts était principalement composé de spécialiste du droit de la sécurité nationale et du droit des conflits armés, et non de spécialistes des droits de l'homme. Elle critique aussi l'approche du *Manuel de Tallinn 2.0* qui se base principalement sur le droit coutumier des droits de l'homme et non sur les nombreux traités existants dans ce domaine. Elle analyse en détail un certain nombre de points problématiques dans le commentaire des règles sur les droits de l'homme. POKEMPNER D., « Squinting through the Pinhole: A Dim View of Human Rights from *Tallinn 2.0* [*Symposium:* Tallinn Manual 2.0 *on the International Law Applicable to Cyber Operations*] », *Texas Law Review*, 2017 2016, vol. 95, p. 1599‑1618.

Voir aussi l'article Rebecca Ingber qui souligne que le chapitre sur les droits de l'homme du *Manuel de Tallinn 2.0* va très certainement s'attirer de nombreuses critiques des universitaires spécialistes des droits de l'homme en ce qu'il reste très général et imprécis, et qu'il laisse une très grande marge d'appréciation aux Etats. INGBER R., « Interpretation Catalysts in Cyberspace », *op. cit.*, p. 1534‑1545. Elle souligne notamment que « [r]ather than provide a bona fide handbook on the application of human rights law to cyberspace, this chapter reads as more of a placeholder. The intimation is: international human rights law is real, it is important, and it regulates state action even in this realm. . . and good luck figuring out how to apply it. » *Ibid.*, p. 1543.

d'expression (commentaire sous la règle 35 – §§2-4, pp. 187-188), le droit à la vie privée (commentaire sous la règle 35 – §§6-15, pp. 189-193), la liberté d'opinion (commentaire sous la règle 35 – §5, p. 188) et le droit au procès équitable (commentaire sous la règle 35 – §§16-18, pp. 193-194). Le groupe d'experts considère que le droit à l'oubli, existant notamment en droit européen, n'a pas valeur coutumière (commentaire sous la règle 35 – §23, pp. 195-196).

Les États ont l'obligation de respecter le droit international des droits de l'homme et de les protéger (règle 36). Le groupe d'experts considère qu'il s'agit d'une obligation coutumière (commentaire sous la règle 36 – §5, p. 198) et qu'elle s'applique donc en ce qui concerne les activités numériques. Cette obligation n'est pas absolue, sauf en ce qui concerne les droits de l'homme absolus, et peut donc connaître certaines limitations (règle 37)[42]. Les droits de l'homme absolus sont par exemple l'interdiction de la torture, de l'esclavage ou encore la liberté d'opinion (commentaire sous la règle 37 – §4, p. 202). De la même manière, les États peuvent déroger aux droits de l'homme, notamment en ce qui concerne les activités numériques, lorsque ces dérogations sont prévues par le traité international concerné (règle 38).

Dans certains cas, l'exercice des droits de l'homme ne peut s'effectuer que par le biais de moyens numériques, par exemple dans le cas où les élections dans un État sont organisées en ligne. Les experts étaient partagés sur le point de savoir si dans ce cas l'Etat a l'obligation de fournir un accès à internet pour permettre aux citoyens de participer aux élections (commentaire sous la règle 36 – §10, pp. 199-200).

3.3.2 Droit diplomatique et consulaire (chapitre 7 – règles 39 à 44)

La coutume internationale en matière de droit diplomatique et consulaire a été codifiée par deux textes : la Convention de Vienne sur les relations diplomatiques[43] et la Convention de Vienne sur les relations consulaires[44]. Les experts chargés de la rédaction du *Manuel de Tallinn* ont basé la plupart des règles en matière diplomatique et consulaire sur ces deux conventions (commentaire introductif du chapitre 7, § 1, p. 209). Le commentaire introductif précise que ce chapitre ne détaille pas le droit applicable aux organisations internationales (commentaire introductif du chapitre 7, § 5, p. 210) et aux missions spéciales (commentaire introductif du chapitre 7, § 6, pp. 210-211).

Les experts ont tenu à rappeler dans le commentaire introductif la relation entre les contre-mesures prévues par le droit de la responsabilité internationale et le droit diplomatique et consulaire : **il est interdit pour un Etat d'adopter des contre-mesures qui violeraient l'inviolabilité des agents, locaux, archives ou documents diplomatiques ou consulaires** (commentaire introductif du chapitre 7, § 8, pp. 211-212).

3.3.2.1 Inviolabilité des systèmes d'information situés dans les locaux diplomatiques et consulaires

La **règle 39 étend l'inviolabilité des locaux diplomatiques et consulaires aux infrastructures numériques qui s'y trouvent**. Les experts considèrent néanmoins que cette règle n'est pas absolue et que l'État accréditaire pourrait prendre certaines mesures contre les

42 Robert E. Barnsby et Shane R. Reeves analysent et critiquent certaines limitations mentionnées dans le commentaire du *Manuel de Tallinn 2.0*, notamment la lutte contre le terrorisme utilisée comme exemple par le groupe d'experts. REEVES S.R. et R.E. BARNSBY, « Give Them an Inch, They'll Take a Terabyte », *op. cit.*, p. 1519‑1523.

43 Convention de Vienne sur les relations diplomatiques, conclue à Vienne le 18 avril 1961, entrée en vigueur le 24 avril 1964, Nations Unies, Recueil des Traités, vol. 500, p. 95.

44 Convention de Vienne sur les relations consulaires, conclue à Vienne le 24 avril 1963, entrée en vigueur le 19 mars 1967, Nations Unies, Recueil des Traités, vol. 596, p. 261.

systèmes d'information concernés dans le cadre de l'exercice de son droit de légitime défense (commentaire sous la règle 39, § 7, p. 214).

L'extension de l'inviolabilité aux systèmes d'information semble assez logique, mais son application pratique a fait débat au sein du groupe d'experts.

Premièrement, les experts étaient d'accord pour dire que **cette règle impose à l'État accréditaire de ne pas violer les locaux et systèmes d'information consulaires ou diplomatiques** (commentaire sous la règle 39, § 3, p. 213). Cependant, une minorité d'experts considèrent que la pénétration exclusivement numérique faite par l'État accréditaire dans les systèmes d'information concernés ne constituerait pas une violation de la règle tant qu'il n'y a pas de dommage physique, puisque la violation des locaux diplomatiques ou consulaires implique une dimension physique (commentaire sous la règle 39, § 4, p. 213). Il s'agit d'une vision minoritaire qui semble assez difficilement soutenable. D'autant qu'aucune disposition du droit international n'impose que la violation soit physique, et donc ne semble justifier la dissociation des violations virtuelles de celles prenant des formes plus traditionnelles. En outre, cette vision reviendrait à dissocier et favoriser l'espionnage conduit par des moyens numériques par rapport aux autres formes d'espionnage.

Deuxièmement, les experts étaient uniformément partagés sur la question de savoir si l'inviolabilité des locaux diplomatiques et consulaires s'appliquait qu'à l'État accréditaire ou aussi aux autres États. En effet, le développement des moyens numériques offre aux Etats de nouveaux moyens pour pénétrer à distance dans des systèmes d'information situés dans d'autres États (commentaire sous la règle 39, § 6, p. 214). Les textes en matière d'inviolabilité des locaux diplomatiques et consulaires ne prévoient que les relations entre l'État accréditant et l'État accréditaire, et ne mentionne les États tiers qu'en ce qui concerne l'inviolabilité des correspondances et communications officielles, reprise dans la règle 41.

Les conventions de Vienne sont antérieures aux développements des systèmes d'information et des moyens permettant de s'y introduire à distance, il semblerait néanmoins étonnant de retenir une interprétation de ces textes permettant aux États tiers de pénétrer et donc d'espionner les ambassades situées à l'étranger en toute impunité. D'autant que les règles sur l'inviolabilité des correspondances et communications officielles émanant des ambassades et consulats situés à l'étranger montrent la volonté des États de prolonger cette inviolabilité dans des cas qui concerneraient des États tiers. Pour ces raisons, il semblerait logique de considérer que l'inviolabilité des systèmes d'information des locaux diplomatiques et consulaires s'applique non seulement aux États accréditaires, mais aussi à tout autre État.

Troisièmement, les experts se sont intéressés au statut des objets liés à la mission diplomatique, mais ne se trouvant pas dans ses locaux, par exemple les téléphones portables et ordinateurs portables des diplomates (commentaire sous la règle 39, § 8-11, p. 215-216). Aucun consensus ne fut trouvé entre les experts : une minorité d'experts considère que ces objets n'étaient pas protégés par cette règle, d'autres experts qu'ils sont protégés dans certaines circonstances, notamment qu'ils ne peuvent faire l'objet d'aucune perquisition, réquisition, saisie ou mesure d'exécution, enfin certains experts considèrent que ces objets sont protégés par cette règle.

Quatrièmement, **les « ambassades virtuelles » établies par certains États n'ont d'ambassade que le nom et ne sont pas couverte par l'inviolabilité des locaux diplomatiques ou consulaires** (commentaire sous la règle 39, § 14, p. 216). De la même manière, l'inviolabilité des locaux diplomatiques ou consulaires ne s'étend pas à leur présence virtuelle sur internet par le biais de sites internet ou de comptes sur des réseaux sociaux (commentaire sous la règle 39, § 15, pp. 216-217), sauf si les données relatives à cette présence en ligne sont stockées sur un système informatique situé dans les locaux de la mission et qui est donc lui-même couvert par l'inviolabilité.

3.3.2.2 Obligations de protéger les infrastructures numériques

L'État accréditaire doit prendre les mesures appropriées pour protéger les infrastructures numériques situées dans les locaux diplomatiques et consulaires contre les dommages ou les intrusions (**règle 40**). Il ne s'agit pas d'une obligation absolue (commentaire sous la règle 40, § 2, p. 217). En effet, il s'agit d'une obligation de moyen et non d'une obligation de résultat.

Cette règle transpose l'article 22(2) Convention de Vienne sur les relations diplomatiques, aux termes duquel *« [l]'État accréditaire a l'obligation spéciale de prendre toutes mesures appropriées afin d'empêcher que les locaux de la mission ne soient envahis ou endommagés, la paix de la mission troublée ou sa dignité amoindrie »*[45].

Le devoir de prendre des mesures pour prévenir les intrusions dans les systèmes concernés découle logiquement de la transposition de l'article 22(2), mais semble poser plusieurs questions pour sa mise en œuvre pratique.

Premièrement, les experts considèrent qu'il n'y a pas d'obligations de prendre des mesures préventives pour protéger les locaux et systèmes d'information concernés tant que l'État accréditaire n'est pas au fait d'une menace particulière (commentaire sous la règle 40, § 4, p. 218).

Deuxièmement, les experts étaient partagés et n'ont pas trouvé de consensus sur la question de savoir si en cas de cyber opérations venant de l'étranger et visant les systèmes d'information concernés, cette règle obligerait l'État accréditaire à chercher l'assistance des États d'origine des cyber opérations. La majorité considérant qu'il n'y a pas d'obligation en ce sens. De notre point de vue, il semblerait plus logique dans ce cas de figure que l'État accréditant soit celui qui cherche l'assistance des États d'origine sur la base des informations transmises par l'État accréditaire au nom de son obligation d'assistance. De même, si on considère que l'État accréditaire n'a pas d'obligation en ce sens, il semblerait logique que dans la mise en œuvre de bonne foi de son obligation de prendre les mesures nécessaires pour protéger les systèmes d'information concernés de se proposer voire de prendre l'initiative de contacter les États d'origine. Il s'agit néanmoins d'un cas de figure difficile à analyser *in abstracto*, en effet, le rôle de chaque État dépendra des circonstances particulières des cyber opérations et seul le développement de la pratique des États pourra établir précisément l'étendue de l'obligation de l'État accréditaire.

3.3.2.3 Inviolabilité des archives, documents et correspondances électroniques

La **règle 41 étend l'inviolabilité des archives, documents et correspondances officiels des missions diplomatiques ou consulaires même lorsqu'ils sont sous forme électronique**. Cette règle s'étend aussi aux documents et communications privées des agents diplomatiques, mais pas à ceux des agents consulaires (commentaire sous la règle 41 – § 5, p. 220). De manière pertinente, le groupe d'expert considère que la protection dont jouissent les archives électroniques s'étend aux supports physiques de ces archives comme les disques durs externes ou les clefs USB (commentaire sous la règle 41 – § 3, p. 220).

Cette règle ne se limite pas à l'État accréditaire, mais concerne tous les États qui ont donc l'obligation de respecter l'inviolabilité des archives, documents et correspondances électroniques concernés lorsqu'ils transitent par leurs infrastructures numériques (commentaire sous la règle 41 – § 7, p. 221). À l'inverse les experts étaient partagés quant à l'inviolabilité pour les États étrangers des données stockées sur des serveurs à l'étranger qui ne sont pas situés dans l'enceinte des locaux diplomatiques ou consulaires (commentaire sous la règle 41 – § 8, pp. 221-222).

Les experts ne purent trouver d'accord sur le contenu et l'étendue de l'interdiction de la surveillance électronique par les États tiers des communications diplomatiques (commentaire

45 Voir aussi l'article 31(3) de la Convention de Vienne sur les relations consulaires.

sous la règle 41 – §§9-11, pp. 222-223). En effet, les communications électroniques des missions diplomatiques sont protégées, mais est-ce que cette protection s'étend seulement à celle avec l'État accréditant ? Celles avec l'État accréditaire ? Celles avec les autres missions diplomatiques présentes sur le territoire de l'État accréditaire ? Ou à toutes leurs communications ? La majorité des experts sont de l'avis que toutes les communications électroniques sont protégées (commentaire sous la règle 41 – §1, pp. 222), ce qui semble être l'approche la plus appropriée, même la pratique étatique montre de nombreux exemples de violation des communications diplomatiques (commentaire sous la règle 41 – §11, p. 223).

Le groupe d'experts souligne qu'il ne semble pas y avoir d'obligation coutumière imposant un marquage spécifique des archives, des documents et des communications officiels des missions diplomatiques et consulaires attestant de leur inviolabilité. Un marquage physique avait été proposé au moment de la négociation sur l'adoption de la Convention de Vienne sur les relations diplomatiques et avait été rejeté (commentaire sous la règle 41 – §17, p. 225). Les arguments avancés par le groupe d'experts sont tout à fait pertinents, il convient par ailleurs d'ajouter qu'un tel marquage numérique pourrait aussi augmenter la vulnérabilité de ces données protégées en permettant de chercher par des moyens numériques toutes les données portant le même marquage. Il ne serait donc pas souhaitable d'instaurer un marquage numérique des données protégées.

3.3.2.4 Libre communication

L'État accréditaire doit permettre et protéger la libre communication de la mission diplomatique ou consulaire pour toutes fins officielles (**règle 42**).

3.3.2.5 Utilisation des locaux diplomatiques et consulaires

La **règle 43(a)** prescrit que **les locaux diplomatiques et consulaires ne seront pas utilisés pour perpétrer des cyber opérations incompatibles avec les fonctions de la mission diplomatique ou consulaire**. La **règle 43(b) étend cette prescription aux agents diplomatiques et personnels consulaires qui ne devraient pas conduire de cyber activités interférant avec les affaires internes de l'État accréditaire ou incompatibles avec le droit national applicable de cet État**.

La règle concerne la conduite de cyber opérations à l'encontre de l'État accréditaire. Néanmoins, le groupe d'experts précise dans le commentaire que les locaux diplomatiques ou consulaires ne peuvent pas servir de base pour lancer des opérations de cyber espionnage à l'encontre d'autres États puisque ce type d'activités seraient incompatibles avec les fonctions de la mission (commentaire sous la règle 43, §4 – p. 229).

Les deux conventions de Vienne sur les relations diplomatiques et consulaires précisent que les missions diplomatiques ou consulaires ne peuvent installer *« un poste émetteur de radio qu'avec l'assentiment de l'État accréditaire »*. Les experts sont néanmoins de l'avis que cette règle ne s'applique pas dans le cas d'un équipement n'émettant qu'à l'intérieur de la mission, comme un par exemple un router Wifi, et que par conséquent ce type d'équipement peut être installé sans l'assentiment de l'État accréditaire (commentaire sous la règle 41, §8 – p. 230).

3.3.2.6 Privilèges et immunités

Les privilèges et immunités dont bénéficient les agents diplomatiques et consulaires s'appliquent aussi à leurs activités numériques (**règle 44**).

3.3.3 Le régime juridique international des espaces : le droit de la mer (chapitre 8 – règles 45 à 54), le droit aérien (chapitre 9 – règles 55 à 57) et le droit spatial (chapitre 10 – règles 58 à 60)

Le régime juridique des espaces détermine un certain nombre de normes spécifiques applicable lorsque les activités prennent place dans les espaces concernés, qu'il s'agisse des mers (chapitre 8), **des airs** (chapitre 9) ou encore de **l'espace extra-atmosphérique** (chapitre 10). La plupart des 16 règles du *Manuel de Tallinn 2.0* en matière de régime juridique des espaces ne sont qu'une transposition des normes existant en droit international et qui sont applicables à toutes activités humaines se déroulant dans ces espaces, y compris les cyber opérations. En effet, le groupe d'experts internationaux a construit les règles énumérées en se basant, dans la plupart des cas, sur les traités internationaux codifiant la coutume internationale applicable en matière de régime des espaces. Ainsi, les règles de droit de la mer reprennent des dispositions de la Convention des Nations unies sur le droit de la mer[46], celles en matière de droit aérien se basent sur Convention relative à l'aviation civile internationale [47]et celles en matière de droit spatial sont inspirées du Traité de l'espace[48] et du Traité sur la Lune[49].

Les normes de droit des espaces reprises par le groupe d'experts font généralement l'objet d'un consensus assez large et l'application de ces normes au domaine numérique ne pose donc pas de problèmes particuliers. Par conséquent, cette analyse se contentera d'un bref résumé de ces normes.

3.3.3.1 Droit de la mer (chapitre 8 – règles 45 à 54)

Dans le cas de **cyber opérations prenant place en mer**, **il conviendra de distinguer que l'on se trouve en haute mer** (**règles 45 et 46**), zone échappant à la souveraineté des États et qui *« est affectée à des fins pacifiques »*[50], **des autres zones où des États exercent leurs juridictions et ont certaines prérogatives : zone économique exclusive** (**règles 46 et 47**), **mer territoriale** (**règles 48, 49 et 50**), **zone contiguë** (**règle 51**), **eaux archipélagiques** (**règle 52**), ou encore les **détroits internationaux** (**règle 53**).

La **règle 46** sur le **droit de visite**, *« **A warship or other duly authorised vessel may exercise the right of visit to board a vessel without flag State consent on the high seas or within an exclusive economic zone if it has reasonable grounds for suspecting the vessel is utilising cyber means to engage in piracy, slave trading, or unauthorised broadcasting; appears to be without nationality; or is of the nationality of the visiting vessel** »*, reprend les dispositions de l'article 110 de la Convention des Nations unies sur le droit de la mer.

Les experts étaient partagés sur la question de savoir si ce droit de visite pouvait se faire de manière virtuelle (commentaire sous la règle 46, §§ 10-11, pp. 238-239) ? En d'autres termes, **ils n'ont pas trouvé de consensus pour déterminer si une visite virtuelle, c'est-à-dire le fait de pénétrer par des moyens numériques dans les systèmes d'information du navire visé pour**

---

46 Convention des Nations unies sur le droit de la mer, adoptée le 16 novembre 1973, entrée en vigueur 16 novembre 1994.

47 Convention relative à l'aviation civile internationale, signée à Chicago le 7 décembre 1944, entrée en vigueur le 4 avril 1947.

48 Traité sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, adopté le 19 décembre 1966 par la Résolution no 2222 de l'Assemblée générale des Nations unies, signé le 27 janvier 1967, entré en vigueur le 10 octobre 1967.

49 Accord régissant les activités des États sur la Lune et les autres corps célestes, adopté le 5 décembre 1979, entrée en vigueur le 11 juillet 1984.

50 Article 88, Convention des Nations unies sur le droit de la mer.

le contrôler, pouvait être considérée comme un exercice licite du droit de visite. Certains experts considèrent qu'il s'agirait d'une forme moins intrusive de visite et qu'elle serait donc compatible avec le droit de visite ; à l'inverse d'autres experts considèrent que le contrôle effectué dans le cadre du droit de visite doit se faire à bord du navire visé et ne peut donc pas de faire par des moyens numériques, considérant qu'il s'agirait d'une forme plus intrusive de contrôle puisqu'elle donnerait accès à d'autres informations que celles normalement recherchées.

De plus, la **règle 54** précise que **le droit international applicable en matière de câbles sous-marins s'applique aux câbles sous-marins de communication**. Les communications, et notamment l'internet mondial, reposent majoritairement sur les communications intercontinentales par le biais de câbles sous-marins. Le droit international en matière de câbles sous-marins a émergé avec le développement des câbles sous-marins télégraphiques, mais les normes développées dans ce contexte sont aussi applicables aux câbles sous-marins à vocation de communications.

3.3.3.2 Droit aérien (chapitre 9 – règles 55 à 57)

En matière de droit aérien, il convient de distinguer les **cyber opérations prenant place dans un espace aérien sous la souveraineté d'un État** (**règle 55**), c'est-à-dire l'espace aérien se trouvant au-dessus de son territoire, ou dans l'**espace aérien international** échappant à la souveraineté des États (**règle 56**).

La **règle 57** est la transposition des articles 3(d) et 3 *bis* de la Convention relative à l'aviation civile internationale. Aux termes de cette règle, **les États doivent s'abstenir de conduire des cyber opérations qui mettraient en péril la sécurité internationale de l'aviation civile**, sauf en cas d'exceptions prévues par le droit international par exemple dans le cadre de l'exercice par un État de son droit de légitime défense (commentaire sous la règle 57, § 2, pp. 268-269).

3.3.3.3 Droit spatial (chapitre 10 – règles 58 à 60)

En matière de droit spatial, **il convient de distinguer les cyber opérations transitant par des moyens spatiaux et ne posant pas de problème particulier en matière de droit spatial, de celles qui sont lancées ou qui visent des systèmes spatiaux** (commentaire introductif du chapitre 10 – §§ 2-3, pp. 270-271). Dans le second cas, les cyber opérations doivent se conformer aux normes de droit spatial applicables.

Les cyber opérations conduite dans l'espace doivent respecter les limitations sur l'usage de la force imposées par le droit international général, notamment la Charte des Nations Unies. Les cyber opérations prenant place sur la Lune ou une autre corps céleste doivent être pacifiques (**règle 58**).

Le régime de responsabilité internationale spécifiquement développé pour les activités spatiales s'applique aussi en ce qui concerne les cyber opérations impliquant des objets spatiaux (**règle 60(b)**). De plus, **les cyber opérations étatiques ayant une dimension spatiale doivent tenir compte de la nécessité d'éviter les gênes potentiellement nuisibles pour les utilisations pacifiques de l'espace faites par d'autres États** (**règle 59(b)**).

L'État sur le registre duquel est inscrit un objet lance dans l'espace extra-atmosphérique conservera sous sa juridiction et son contrôle ledit objet (**règle 59(a)**). Par ailleurs, **l'État est responsable internationalement des activités nationales dans l'espace extra-atmosphérique** ; ainsi, les activités des entités non gouvernementales doivent faire l'objet d'une autorisation et d'une surveillance de la part de l'État (**règle 60(a)**).

3.3.4 Droit international des télécommunications (Chapitre 11 – règles 61 à 64)

Il existe un lien plus qu'étroit et évident entre cyber opérations et télécommunications, et il est donc parfaitement logique que le groupe d'experts du *Manuel de Tallinn* ait décidé de dédier un chapitre au droit international des télécommunications.

La majorité des règles établies par le groupe d'experts sont basées sur les textes de l'Union internationale des télécommunications[51]. Il convient de noter que la transposition de ces règles aux domaines numériques se fait assez naturellement et ne pose donc pas de problèmes particuliers.

La **règle 61** transpose certaines dispositions de l'article 38 de la Constitution de l'UIT. Aux termes de cette règle, **les États doivent prendre les mesures utiles pour l'établissement d'infrastructures de télécommunications internationales nécessaires pour assurer l'échange rapide et ininterrompu des télécommunications internationales. Les États établissant ces infrastructures doivent prendre les mesures nécessaires pour la maintenance et la sauvegarde de ces infrastructures**.

La **règle 62** sur l'arrêt et la suspension des communications numériques reprend les dispositions des articles 35 et 34(2) de la Constitution de l'UIT. **Les États peuvent suspendre le service international de télécommunication, de manière générale ou partielle, sur leur territoire, et doivent en aviser immédiatement les autres Etats** (**règle 62(a)**). **Les États peuvent interrompre les transmissions privées numériques qui sont contraires à leur droit national, à l'ordre public ou aux bonnes mœurs, ou qui peuvent paraître dangereuses pour la sûreté de l'État** (**règle 62(b)**).

La **règle 63** reprend l'interdiction de l'article 45 de la Constitution de l'IUT d'utiliser des stations d'une manière qui causerait des **brouillages préjudiciables aux communications ou services radioélectriques d'autres États,** et l'étend aux brouillages des fréquences utilisées pour communications ou services numériques sans fil.

La **règle 64** rappelle l'entière **liberté des États en ce qui concerne les installations radioélectriques militaires** prévue par l'article 48(1) de la Constitution de l'IUT.

---

51 UNION INTERNATIONALE DES TELECOMMUNICATIONS, *Recueil des textes fondamentaux de l'Union internationale des télécommunications adoptés par la Conférence de plénipotentiaires*, 2015, disponible en ligne: http://handle.itu.int/11.1002/pub/80a4dff8-en.

3.4 Paix et la sécurité internationales et cyber activités (Part III. International peace and security and cyber activities – pp. 301 à 371 – règles 65 à 79)

La troisième partie du *Manuel de Tallinn 2.0* fait la transition entre les nouvelles règles adoptées pour la seconde édition du *Manuel de Tallinn* et celles reprises de la première édition. En effet, les deux premiers chapitres de cette partie sont nouveaux alors que le troisième chapitre est repris de la première édition, dans laquelle il était le second chapitre de la première partie.

3.4.1 Règlement pacifique des différends (chapitre 12 – règle 65)

La **règle 65** traite de la question du règlement pacifiques des différends, et comporte deux alinéas :

> **(a) Les Etats doivent chercher à régler leurs différends impliquant des activités numériques internationaux mettant en danger la paix et la sécurité internationales par des moyens pacifiques ;**
> **(b) Si les États cherchent à régler leurs différends impliquant des activités numériques qui ne mettent pas en danger la paix et la sécurité internationales, ils doivent le faire par des moyens pacifiques.**

Les deux alinéas de la règle 65 peuvent paraître similaires, mais comportent une différence notable. Dans le premier cas, lorsqu'il s'agit d'un différend mettant en danger la paix et la sécurité internationales, les États sont obligés de chercher à le régler par des moyens pacifiques. Dans le second cas, lorsque le différend en question ne met pas en danger la paix et la sécurité internationales, les Etats n'ont pas d'obligation de chercher à le régler, mais s'ils le font, ils doivent le faire par des moyens pacifiques (§§ 15-23, pp.308-310).

Cette règle est construire sur la base de différentes normes de droit coutumier, de décisions de la CIJ et de résolutions de l'Assemblée générale des Nations Unies (commentaire sous la règle 65 – §1, p. 303). Sa rédaction est inspirée des articles 2(3) et 33(1) de la Charte des Nations Unies (§ 2, p. 303).

3.4.2 Interdiction de l'intervention (chapitre 13 – règle 66 et 67)[52]

3.4.2.1 Interdiction de l'intervention par les États (règle 66)

Un État ne doit pas intervenir, notamment par des moyens numériques, dans les affaires intérieures ou extérieures d'un autre État (**règle 66**).

Cette règle reprend le principe de non-intervention du droit international coutumier qui a été rappelé par la CIJ dans l'affaire *Nicaragua*, par plusieurs déclarations et traités internationaux et dans plusieurs résolutions de l'Assemblée générale des Nations Unies. Le principe de non-intervention est un des corolaires de l'égalité souveraine des Etats (commentaire sous la règle 66 – §1, p.312-313). La CIJ, dans l'affaire *Nicaragua,* a précisé que de nombreux exemples de violations du principe de non-intervention existaient dans la pratique des États, mais que cela n'affectait pas l'existence du principe coutumier de non-intervention[53]. Ce principe ne concerne

---

52 Michael N. Schmitt a publié un article où il revient sur les différents points abordés dans les deux éditions du *Manuel de Tallinn* et qui mériteraient d'être étudiés plus en avant, notamment le principe de non-intervention. SCHMITT M.N., « Grey Zones in the International Law of Cyberspace », *op. cit.*, p. 7‑8.

53 *Nicaragua* (fond), *op. cit.*, p. 98, para 186 et pp. 107‑108, para 205.

que les relations interétatiques, et donc les interventions potentielles d'un État dans les affaires d'un autre État (§4, pp.313-314).

Selon le groupe d'experts, une intervention illicite est caractérisée par deux éléments : premièrement, l'acte en question doit être relatif aux affaires intérieures ou extérieures de l'État visé ; deuxièmement, cet acte doit être coercitif, c'est-à-dire qu'il doit avoir pour objectif à contraindre l'État visé (§ 6, p. 314). Cette approche est séduisante, mais il nous semble pertinent d'ajouter un premier élément, mentionné précédemment dans le commentaire, mais non repris comme un élément constitutif d'une intervention illicite, à savoir le caractère interétatique de l'acte. Ainsi, **les trois éléments constitutifs d'une intervention illicite sont :**

1. **Un acte d'un État contre un autre État ;**
2. **Visant à contraindre l'État visé ;**
3. **Relatif aux affaires intérieures ou extérieures de l'État visé.**

Comme le précise la CIJ, *« [l]'intervention interdite doit donc porter sur des matières à propos desquelles le principe de souveraineté des États permet à chacun d'entre eux de se décider librement. Il en est ainsi du choix du système politique, économique, social et culturel et de la formulation des relations extérieures »*[54]. Le commentaire analyse longuement les matières concernées (§§ 8-16, pp. 315-317), nous ne reviendrons pas sur cette analyse dans la présente note.

L'élément de contrainte de l'intervention illicite n'a pas besoin d'être physique (§ 20, p. 318). Par conséquent, **la contrainte d'un État exercée sur un autre État par des moyens numériques pourra aussi constituer une forme illicite d'intervention**. **La contrainte peut être exercée directement ou indirectement** (§ 23, p. 319). **Les experts considèrent que la seule menace peut suffire à constituer une intervention illicite** (§ 30, p. 322-323).

Les experts sont divisés sur la question de savoir si l'État visé doit être au courant de la cyber opération pour qu'elle constitue une intervention illicite (§ 25, pp. 320-321). La majorité des experts considère que la connaissance de la cyber opération n'est pas une précondition pour cette règle. Une minorité d'experts considère que c'est un élément décisif, car si l'Etat n'a pas connaissance de l'acte visant à le contraindre, il ne peut donc pas y avoir de contrainte exercée par un Etat sur un autre État. La majorité des experts considère néanmoins que même si l'État visé n'a pas connaissance de l'acte en question, il peut cependant être contraint par ses effets et que donc l'élément de contrainte est bien présent.

Les experts reviennent à nouveau sur la question de l'espionnage, qui a déjà été abordée à plusieurs reprises dans le *Manuel de Tallinn 2*.0. Ils considèrent que l'espionnage numérique n'est pas une forme d'intervention illicite, car il manque l'élément de contrainte (§ 33, p. 323).

Les mesures numériques dont l'objet est économique ont retenu l'attention du groupe d'experts. Ces mesures peuvent par exemple prendre la forme pour un État de bloquer l'accès d'un site de e-commerce à un autre État ou encore de lui bloquer l'accès à des serveurs qu'il utilise et qui sont situés sur le territoire de l'État qui prend la mesure. Les experts considèrent que ces mesures ne constitueraient pas des interventions illicites (§ 35, p. 324).

3.4.2.2 Interdiction de l'intervention par l'Organisation des Nations Unies (règle 67)

La **règle 67** reprend l'article 2(7) de la Charte des Nations Unies et précise que **l'Organisation des Nations Unies n'est pas autorisée à intervenir, notamment par des moyens numériques, dans des affaires qui relèvent essentiellement de la compétence nationale d'un État, mais que néanmoins ce principe ne porte en rien atteinte à l'application des**

54 *Nicaragua* (fond), *op. cit.*, p. 108, para 205.

mesures de coercition décidées par le Conseil de sécurité des Nations Unies sur la base du Chapitre VII de la Charte des Nations Unies.

La majorité des experts estime que cette règle ne vaut que pour les Nations Unies et qu'il n'existe pas de norme de droit international coutumier étendant ce principe aux autres organisations internationales (commentaire sous la règle 67 – §1, p. 325). Cette assertion est étonnante puisque dans le commentaire introductif de la section sur la responsabilité des organisations internationales, les experts précisent que « [t]he international group of Experts agreed that international organisations are subject to the prohibition of intervention (Rule 66) a conclusion supported, in part, by the prohibition of United Nations intervention set forth in Article 2(7) of the UN Charter (Rule 67) » (commentaire introductif – §10, p. 156). Il est donc surprenant de voir qu'à la page 156, les experts considèrent que le principe de non-intervention s'applique aux organisations internationales et de voir la majorité d'entre-deux rejeter cette applicabilité à la page 325.

4 Les règles du Manuel de Tallinn 2.0 reprises de la première édition

A partir du Chapitre 14 (p. 327), le *Manuel de Tallinn 2.0* reprend les règles et commentaires de la première édition du *Manuel de Tallinn* publiée en 2013, avec quelques modifications et mises à jour. Les anciennes règles du *Manuel de Tallinn 1.0* sont reprises dans deux parties : la troisième partie sur la paix et la sécurité internationales et cyber activités et la quatrième partie sur le droit des cyber conflits armés.

La troisième partie du *Manuel de Tallinn 2.0* se compose de règles et commentaires nouveaux et d'autres issus de la première édition du *Manuel de Tallinn*. Ainsi, les chapitre 12 sur le règlement pacifique des différends (règle 65) et le chapitre 13 sur l'interdiction de l'intervention (règles 66 et 67) sont des ajouts alors que le chapitre 14 sur le recours à la force (règles 68 à 75) et le chapitre 15 sur la sécurité collective (règle 76 à 79) sont repris de la première édition.

Il a été décidé dans le cadre de cette analyse de résumer et analyser les règles relatives au recours à la force et la sécurité collective, pour faire le lien avec le reste de la troisième partie, mais pas les règles de la quatrième partie sur le droit des cyber conflits armés.

4.1 Paix et la sécurité internationales et cyber activités [*suite*] (pp. 327 à 371 – règles 68 à 79)

4.1.1 Le recours à la force (chapitre 14 – règle 68 et 75)

Le chapitre 14 sur le recours à la force se découpe en deux sections, la première sur l'interdiction du recours à la menace ou à l'emploi de la force et la seconde sur la légitime défense. Les huit règles concernées (règles 68 à 75) reprennent mot pour mot les règles de la première édition (règle 10 à 17).

Dans l'introduction du chapitre 14, le groupe d'experts rappelle que la Cour international de Justice a précisé que les articles 2, paragraphe 4, et 51 de la Charte des Nations Unies, qui traitent respectivement de l'interdiction du recours à la menace ou à l'emploi de la force et de la légitime défense, s'appliquent « *à n'importe quel emploi de la force, indépendamment des armes employées* »[55]. Le groupe d'experts précise être d'accord avec cette affirmation et reconnait son caractère coutumier. Par conséquent, une cyber opération peut constituer un recours à la menace ou à l'emploi de la force ou un agression armée ouvrant le droit pour l'Etat victime d'invoquer la légitime défense (commentaire introductif du chapitre 14 – § 1, p. 329).

Le groupe d'experts précise que la pratique étatique est encore naissante quant à l'application du *jus ad bellum* aux cyber opérations, et qu'il n'existe à l'heure actuelle pas de consensus sur les définitions, les critères et les seuils d'applicabilité engendrant ainsi une certaine forme d'incertitude sur les modalités pratiques d'application du *jus ad bellum* dans ce contexte. Il précise que les règles et commentaires contenus dans le *Manuel de Tallinn 2.0* se basent sur la *lex lata*, mais que les cyber opérations constituent un enjeu grandissant et évolutif pour le droit international et que son contenu ou son interprétation pourrait évoluer en conséquence (commentaire introductif du chapitre 14 – § 3, pp. 328-329).

55 *Licéité de la menace ou de l'emploi d'armes nucléaires* (avis consultatif), 1996, p. 244, para 39.

4.1.1.1 Interdiction du recours à la force (chapitre 14, section 1 – règles 68 à 70)

La **règle 68** se base sur l'article 2, paragraphe 4, de la Charte des Nations Unies[56] et précise qu'**une cyber opération qui constitue un recours à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies, est illicite**.

Le commentaire précise que pour constituer un recours à la menace ou à l'emploi de la force, une cyber opération ne doit pas nécessairement être le fait des forces armées de l'Etat. Une cyber opération menée par une agence de renseignement ou une entité non-étatique agissant pour le compte de l'Etat pourrait tout aussi bien constituer un recours à la menace ou à l'emploi de la force (commentaire sous la règle 68 – §4, p. 330).

L'interdiction du recours à la menace ou à l'emploi de la force fait partie tant du droit écrit (article 2, paragraphe 4, de la Charte des Nations Unies) que du droit coutumier, et s'applique donc aussi aux Etats non-membres des Nations Unies. A l'inverse, **cette interdiction ne s'applique pas aux acteurs non-étatiques** (commentaire sous la règle 68 – §5, p. 330).

Les règles 69 et 70 visent respectivement à définir les notions d'emploi de la force et de recours à la menace d'emploi de la force.

4.1.1.1.1 L'interdiction de l'emploi de la force

La **règle 69** définit la notion d'emploi de la force, en précisant qu'**une cyber opération constitue un emploi de la force quand son ampleur et ses effets sont comparables à ceux d'une d'un emploi de la force non numérique**. La règle 69 est donc construite par analogie, une cyber opération constitue un emploi de la force dès lors que ses effets et son ampleur sont équivalent à ceux d'un emploi de la force dans le monde réel.

Le groupe d'experts rappelle que la Charte des Nations Unies ne donne aucun critère pour la définition de l'emploi de la force. **Les deux critères utilisés dans la règle 69, à savoir « l'ampleur » et « les effets », ont été repris du jugement de la CIJ dans l'affaire *Nicaragua* [57], qui les avait utilisés pour la détermination de la survenance d'une agression armée** (commentaire sous la règle 69 – §1, pp. 330-331). Le groupe d'experts voit dans ces critères un moyen de prendre en compte à la fois les aspects quantitatifs et qualitatifs des cyber opérations concernées.

Les paragraphes 2 à 4 rappellent qu'il n'y a pas de définition de la force. Ils font référence aux travaux préparatoires de la Charte des Nations Unies et aux exemples de l'affaire *Nicaragua*. Dans l'affaire Nicaragua, la CIJ a précisé que :

> « Selon la Cour, si le fait d'armer et d'entraîner les *contras* peut assurément être considéré comme impliquant l'emploi de la force contre le Nicaragua, il n'en va pas forcément de même pour toutes les formes d'assistance du Gouvernement des Etats-Unis. La Cour considère en particulier que le simple envoi de fonds aux *contras*, s'il constitue à coup sûr un acte d'intervention dans les affaires intérieures du Nicaragua [...] ne représente pas en lui-même un emploi de la force »[58].

Sur cette base, le groupe d'experts considère que la fourniture par un Etat à un groupe armé d'un virus informatique et de la formation nécessaire pour pouvoir l'utiliser contre un autre Etat,

---

56 Article 2, paragraphe 4, de la Charte des Nations Unies : « *Les Membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies.* »

57 *Nicaragua* (fond), *op. cit.*, p. 103‑104, para 195.

58 *Ibid.*, p. 119, para 228.

pourrait être considéré comme un emploi de la force par analogie avec le jugement de la CIJ dans l'affaire *Nicaragua*. Il est précisé que cette situation doit être distinguée de celle où les actes d'un groupe armé sont imputables à l'Etat aux termes du droit de la responsabilité internationale de l'Etat (commentaire sous la règle 69 – §4, pp. 331-332).

Dans le paragraphe 5, le groupe d'experts s'interroge sur le cas d'un Etat offrant un sanctuaire à un groupe armé lui permettant de conduire des cyber opérations atteignant le seuil d'intensité et d'effets du recours à l'emploi de la force contre un autre Etat depuis son territoire. Les experts étaient partagés sur ce cas, seule une minorité considère qu'il pourrait s'agir d'un recours à l'emploi de la force de la part de l'Etat permettant l'usage de son territoire. A l'inverse, il y a consensus parmi les experts sur le fait que cette situation puisse, sous certaines conditions, constituer une violation de l'obligation de diligence de l'Etat permettant l'usage de son territoire (règles 6 et 7).

Le groupe d'experts rappelle que la CIJ, dans l'affaire *Nicaragua*, a précisé « [qu'] *il y aura lieu de distinguer entre les formes les plus graves de l'emploi de la force (celles qui constituent une agression armée) et d'autres modalités moins brutales* »[59]. Il est intéressant de noter que le groupe d'experts en tire une conclusion dont la formulation peut sembler curieuse : « *The International Group of Experts agreed, therefore, that any cyber operation that rises to the level of an 'armed attack' in terms of scale and effects pursuant to Rule 71, and that is conducted by or otherwise attributable to a State, qualifies as a 'use of force'* » (commentaire sous la règle 69 – §6, p. 332). Ainsi, au lieu de réaffirmer la distinction entre le seuil du recours à l'emploi de la force et celui de l'agression armée, ce dernier étant une sous-catégorie du précédant puisqu'il ne concerne que « *les formes les plus graves de l'emploi de la force* » d'après la CIJ, les experts ont préféré rappeler toutes les agressions armées constituent aussi des emplois de la force. On peut s'interroger sur le choix de la formulation de ce paragraphe qui peut sembler floue et qui semble atténuer l'écart entre les deux seuils.

Dans cette perspective, le paragraphe suivant vient rappeler la position des Etats-Unis sur ce point, sans qu'elle soit endossée par le groupe d'experts, affirmée à l'occasion de l'affaire Nicaragua, selon laquelle l'écart entre les seuils de l'emploi de la force et de la légitime défense serait insignifiant et que donc tout emploi de la force constituerait aussi une agression armée ouvrant la possibilité de l'invocation du droit de légitime défense (commentaire sous la règle 69 – §7, pp. 332-333).

Dans le paragraphe final du commentaire sous la règle 69 (§11, p. 337), les experts rappellent la distinction entre l'emploi de la force et l'agression armée et que l'Etat victime d'un emploi de la force ne constituant pas une agression armée ne pourra pas invoquer son droit de légitime défense et ne pourra donc y répondre que par des contre-mesures (règle 20) ou des mesures justifiées par l'invocation de l'état de nécessité (règle 26).

Certaines cyber opérations pourraient donc constituer un emploi de la force sans pour autant atteindre le seuil de l'agression armée, **le groupe d'experts s'interroge sur les critères à utiliser pour déterminer dans quel cas une cyber opération pourrait constituer un emploi de la force. Pour ce faire, le groupe d'experts reprend les critères proposés par Michael N. Schmitt, le directeur du *Tallinn Manuel Process* et des deux éditions du *Manuel de Tallinn*, dans un article paru en 1999**[60] (commentaire sous la règle 69 – §§8-10, pp. 333-337).

Les huit facteurs sont :

1. **Le degré de gravité de la cyber opération**. Les cyber opérations qui causent des dommages physiques, des blessures voire la mort d'individus constituent des recours à la

59 *Ibid.*, p. 101, para 191.

60 SCHMITT M.N., « Computer network attack and the use of force in international law: thoughts on a normative framework », *Columbia Journal of Transnational Law*, 1999, vol. 37, p. 914.

force. La qualification des cyber opérations ne causant pas de dommage physique n'est pas clairement arrêtée et il difficile de déterminer précisément le seuil.

2. **Le caractère immédiat de la cyber opération**.
3. **Le caractère direct ou non de la cyber opération**, c'est-à-dire le lien de causalité entre la cyber opération et ses effets.
4. **Le degré d'intrusion de la cyber opération** dans les systèmes de l'Etat victime. Par exemple, aux termes de ce critère, la pénétration dans un système informatique militaire hautement sécurisé est considérée comme plus intrusive que celle dans le système peu sécurisé d'une petite entreprise. Le commentaire précise que dans le cas de cyber opérations visant des noms de domaine, celles visant des noms de domaine d'Etat ou de leurs organes en particulier seront considérées comme plus intrusives que celles visant des domaines qui ne sont pas liés à un Etat en particulier, citant comme exemple le nom de domaine « .com ». Encore une fois, le commentaire revient sur le cas de l'espionnage en reprécisant qu'il n'est pas illicite *per se* et que des actes d'espionnage numérique particulièrement intrusifs ne constitueraient pas systématiquement des emplois de la force, tout en précisant néanmoins que certains actes d'espionnage numériques pourraient être des emplois de la force.
5. **Caractère mesurable des effets de la cyber opération**.
6. **Caractère militaire de la cyber opération**.
7. **Degré d'implication d'un Etat dans la cyber opération**.
8. **Présomption de licéité.** Ce dernier critère se base sur le célèbre *dictum* de la Cour permanente de Justice internationale dans l'affaire du *Lotus* qui est généralement interprété comme affirmant que tout ce qui n'est pas interdit en droit international est permis : « *Le droit international régit les rapports entre des Etats indépendants. Les règles de droit liant les Etats procèdent donc de la volonté de ceux-ci, volonté manifestée dans des conventions ou dans des usages acceptés généralement comme consacrant des principes de droit et établis en vue de régler la co-existence de ces communautés indépendantes ou en vue de la poursuite de buts communs. Les limitations de l'indépendance des Etats ne se présument donc pas.* »[61]. Ainsi, des types d'actes qui ne sont pas expressément reconnus comme illicites par un traité ou la coutume internationale, seraient licites et, par conséquence, moins susceptibles de constituer un emploi de la force. Cette analyse peut sembler curieuse en ce qu'il n'existe en droit international pas de lien de causalité entre la licéité ou non d'un acte au regard du reste du droit international et sa qualification comme recours illicite à l'emploi de la force.

Le commentaire précise que cette approche et donc ces facteurs mettent l'accent sur la gravité du préjudice infligé et sur certains facteurs qualitatifs. Cette approche vise principalement à identifier les cyber opérations qui seraient équivalentes à d'autres types d'opérations généralement considérés comme des emplois de la force, et donc remplissant les critères d'ampleur et d'effets développés précédemment. Finalement, il est précisé qu'il s'agit de facteurs qui ont une influence dans la qualification d'un acte donné comme emploi de la force par un Etat mais qu'il ne s'agit pas de critères juridiques (§9, p. 333). De plus, cette liste de facteurs n'est pas exhaustive et d'autres facteurs peuvent être pris en compte, citant en exemple la nature de la cible, l'identité de l'attaquant ou encore le contexte géopolitique préexistant (§10, p. 337).

4.1.1.1.2 L'interdiction du recours à la menace d'emploi de la force

La **règle 70** revient sur la définition de l'interdiction du recours à la menace d'emploi de la force, et précise qu'**une cyber opération, ou la menace d'une cyber opération, constitue une menace illicite à l'emploi de la force à partir du moment où l'action menacée, si elle était mise en œuvre, constituerait un recours illicite à l'emploi de la force**.

61 *Affaire du « Lotus »*, 1927, vol.Serie A, N°10, p. 18.

La formulation de cette règle reprend l'approche suivie par la CIJ dans l'avis consultatif sur les armes nucléaires :

> « La question de savoir si une intention affichée de recourir à la force, dans le cas où certains événements se produiraient, constitue ou non une « menace » au sens de l'article 2, paragraphe 4, de la Charte est tributaire de divers facteurs. Si l'emploi de la force envisagé est lui-même illicite, se déclarer prêt à y recourir constitue une menace interdite en vertu de l'article 2, paragraphe 4. Ainsi serait-il illicite pour un Etat de menacer un autre Etat de recourir à la force pour obtenir de lui un territoire ou pour l'obliger à suivre ou à ne pas suivre certaines orientations politiques ou économiques. Les notions de « menace » et d'« emploi » de la force au sens de l'article 2, paragraphe 4, de la Charte vont de pair, en ce sens que si, dans un cas donné, l'emploi même de la force est illicite - pour quelque raison que ce soit - la menace d'y recourir le sera également. En bref, un Etat ne peut, de manière licite, se déclarer prêt à employer la force que si cet emploi est conforme aux dispositions de la Charte. »[62].

Cette règle distingue deux situations. D'un côté, le cas où la menace d'emploi de la force résulte d'une cyber opération visant à communiquer que l'Etat auteur est prêt à recourir à la force, sous forme numérique ou non. En d'autres termes, cette cyber opération constitue une forme de sommation annonciatrice d'un emploi de la force à venir. D'un autre côté, la menace formulée par tout moyen de recourir à une cyber opération constituant un emploi de la force (commentaire sous la règle 70 – §2, p. 338). Ce second cas prend la plupart du temps la forme d'un ultimatum.

Le commentaire précise que le groupe d'experts était divisé sur le cas particulier d'un Etat qui menace de recourir à l'emploi de la cyber force mais qui ne dispose manifestement pas des capacités nécessaires pour mettre en œuvre cette menace (commentaire sous la règle 70 – §5, p. 339). De la même manière, il n'y avait pas de consensus parmi les experts sur le cas particulier d'un Etat qui menace de recourir à l'emploi de la cyber force mais qui n'a clairement pas l'intention de mettre à exécution cette menace (§6, p. 339).

Il est intéressant de noter que les experts du *Manuel de Tallinn* se sont limités à la menace d'emploi de la force et n'ont pas analysé les autres formes possibles de menace, comme par exemple la démonstration de force. En effet, une partie de la doctrine considère la démonstration de force peut être vue dans certains cas comme une forme de menace d'emploi de la force visant à montrer la détermination de l'Etat à employer la force contre un autre Etat[63].

4.1.1.2 Légitime défense (chapitre 14, section 2 – règles 71 à 75)

La seconde section du chapitre 14 s'intéresse à la légitime défense et comprend cinq règles. La plupart d'entre elles sont basées sur l'article 51 de la Charte des Nations Unies[64] et sur les différentes interprétations que les Etats, la CIJ et la doctrine ont adoptées au regard du droit de légitime défense.

---

62 *Licéité de la menace ou de l'emploi d'armes nucléaires* (avis consultatif), *op. cit.*, p. 246, para 46.

63 Voir notamment : STÜRCHLER N., *The Threat of Force in International Law*, Cambridge University Press, 2007, p. 172-217 ; GRIMAL F., *Threats of Force: International Law and Strategy*, Routledge, 2012, p. 43-46.

64 Article 51 de la Charte des Nations Unies : « *Aucune disposition de la présente Charte ne porte atteinte au droit naturel de légitime défense, individuelle ou collective, dans le cas où un Membre des Nations Unies est l'objet d'une agression armée, jusqu'à ce que le Conseil de sécurité ait pris les mesures nécessaires pour maintenir la paix et la sécurité internationales. Les mesures prises par des Membres dans l'exercice de ce droit de légitime défense sont immédiatement portées à la connaissance du Conseil de sécurité et n'affectent en rien le pouvoir et le devoir qu'a le Conseil, en vertu de la présente Charte, d'agir à tout moment de la manière qu'il juge nécessaire pour maintenir ou rétablir la paix et la sécurité internationales.* »

La **règle 71** applique le droit de légitime défense dans le contexte numérique : **un Etat victime d'une cyber opération dépassant le seuil de l'agression armée peut exercer son droit naturel de légitime défense. La détermination de si une cyber opération constitue une agression armée dépend de son ampleur et de ses effets**.

Le groupe d'experts reconnait unanimement qu'une cyber opération pourrait atteindre le seuil de l'agression armée et donc ouvrir la possibilité pour l'Etat victime d'invoquer son droit de légitime défense (commentaire sous la règle 71 – §4, p. 340). Le groupe d'experts rappelle en ce sens que la CIJ, dans l'avis consultatif sur les armes nucléaires, a indiqué concernant les dispositions de la Charte des Nations Unies sur le recours à la force et la légitime défense qu'elles « *s'appliquent à n'importe quel emploi de la force, indépendamment des armes employées* »[65]. Les experts soulignent, par ailleurs, que cette approche est largement acceptée dans la pratique des Etats.

Le *Manuel de Tallinn 2.0* reprend l'approche traditionnelle selon laquelle les notions d'« emploi de la force » et d'« agression armée » sont distinctes, rappelant la position de la CIJ, exprimée dans l'affaire Nicaragua, selon laquelle « *il y aura lieu de distinguer entre les formes les plus graves de l'emploi de la force (celles qui constituent une agression armée) et d'autres modalités moins brutales* »[66] (commentaire sous la règle 71 – §§6-7, p. 341). Le *Manuel de Tallinn 2.0* reprend les deux critères utilisés par la CIJ dans l'affaire *Nicaragua* [67], à savoir « l'ampleur » et « les effets » (commentaire sous la règle 71 – §7, p. 341). Ces deux critères ont aussi été utilisés par les experts du *Manuel de Tallinn 2.0* pour la détermination de l'occurrence d'un emploi de la force (commentaire sous la règle 69 – §1, pp. 330-331) et ont déjà été commentés précédemment.

Le groupe d'experts souligne que ni la Charte des Nations Unies, ni la jurisprudence de la CIJ, ne fournissent d'instructions claires et précises pour l'agression armée. Les experts affirment qu'une cyber opération qui provoquerait des blessures graves, tuerait un certain nombre d'individus ou causerait des dommages ou destructions physiques importants sur des biens remplirait les critères d'ampleur et d'effets et pourrait donc constituer une agression armée. **Ils citent en exemple le cas de Stuxnet, qui est unanimement considéré par les experts du *Manuel de Tallinn 2.0* comme un emploi de la force mais, à l'inverse, seuls certains experts considèrent qu'il s'agit d'une agression armée** (commentaire sous la règle 71 – §10, p. 342). A l'inverse, ils soulignent que le cas de cyber opérations n'ayant pas d'effets physiques mais ayant néanmoins des conséquences négatives importantes est plus complexe. Une partie des experts considère que la survenance de dommage physique (destruction, blessures ou mort d'individus) est une condition nécessaire pour l'agression armée (commentaire sous la règle 71 – §12, p. 342-343).

Les experts reprennent la théorie de l'accumulation des effets, et reconnaissent ainsi qu'une agression armée peut être constituée de plusieurs actes qui, si analysés séparément, n'atteindraient pas le seuil de l'agression armée (commentaire sous la règle 71 – §11, p. 342).

Le lien de causalité entre la cyber opération et ses effets doit être pris en compte dans la détermination de la survenance d'une agression armée. Le groupe d'experts considère que tous les effets raisonnablement prévisibles doivent être pris en compte (commentaire sous la règle 71 – §13, p. 343).

Le groupe d'experts est divisé sur la question de la prise en compte de l'intention. La majorité des experts sont de l'avis que l'intention n'est pas un critère pertinent et que donc les effets doivent être pris en compte qu'ils soient intentionnels ou non (commentaire sous la règle 71 – §14, pp. 343-344). Il est intéressant de noter que l'exemple utilisé pour illustrer la position des experts qui considèrent que l'intention doit être prise en compte concerne l'espionnage, et semble encore une fois lié au flou qui existe dans les commentaires du *Manuel de Tallinn 2.0* sur la licéité de

65 *Licéité de la menace ou de l'emploi d'armes nucléaires* (avis consultatif), *op. cit.*, p. 244, para 39.

66 *Nicaragua* (fond), *op. cit.*, p. 101, para 191.

67 *Ibid.*, p. 103‑104, para 195.

l'espionnage : « *For instance, consider the example of cyber espionage by one State against another that unexpectedly results in significant damage to the latter's cyber infrastructure. Some of the Experts were unwilling to characterise the operation as an armed attack because the consequences are unintended, although they acknowledged that measures could be taken to counteract the negative effects of the operation (e.g., the plea of necessity discussed in Rule 26)* » (§14, p. 343). Dans la continuité de la discussion sur l'intention, le *Manuel* analyse la question des effets sur les Etats tiers et s'interroge sur leur possible qualification comme agression armée par l'Etat tiers victime. La majorité des experts considère que si l'intensité et les effets de cette cyber opération pour l'Etat tiers atteignent le seuil de l'agression armée, alors il pourra invoquer son droit de légitime défense (commentaire sous la règle 71 – §15, p. 344). Une minorité d'experts considère qu'il ne peut s'agir d'une agression armée du fait de l'absence d'intention de la part de l'Etat auteur de viser l'Etat tiers.

Une question importante concernant la détermination de la survenance d'une agression armée concerne son auteur. Il est indiscutable que les actes des Etats et de leurs organes, ainsi que ceux de groupes non-étatiques agissant pour leur compte et qui leur sont attribuables, peuvent constituer une agression armée (commentaire sous la règle 71 – §16-17, pp. 344). Le Manuel cite en ce sens la CIJ dans l'affaire Nicaragua :

> « En particulier, on peut considérer comme admis que, par agression armée, il faut entendre non seulement l'action des forces armées régulières à travers une frontière internationale mais encore « l'envoi par un Etat ou en son nom de bandes ou de groupes armés, de forces irrégulières ou de mercenaires qui se livrent à des actes de force armée contre un autre Etat d'une gravité telle qu'ils équivalent » (entre autres) à une véritable agression armée accomplie par des forces régulières, « ou [au] fait de s'engager d'une manière substantielle dans une telle action » »[68].

A l'inverse, **la question de savoir si les actes d'un groupe non-étatique n'agissant pas pour le compte d'un Etat et non attribuables à un Etat peuvent constituer une agression armée est plus controversée** (commentaire sous la règle 71 – §§18-20, pp. 345-346). Traditionnellement, le droit international de la légitime défense ne reconnait que les actes des Etats comme pouvant constituer potentiellement des agressions armées. Néanmoins, le *Manuel de Tallinn* analyse l'évolution de la pratique des Etats, citant notamment le cas des attentats du 11 septembre 2001, et souligne la volonté de certains Etats de pouvoir invoquer le droit de légitime défense contre des acteurs non-étatiques sans lien avec un Etat. Il note que la CIJ semble opposée à cette évolution (§18, p. 345). **La majorité des experts considère qu'il existe une pratique suffisante pour conclure que le droit de légitime défense peut être invoqué contre un acteur non-étatique sans lien avec un Etat, notamment contre des groupes terroristes ou rebelles** (§19, p. 345).

Dans le cas d'une agression armée lancée depuis le territoire d'un Etat sans que celui-ci soit au courant, il est nécessaire de prendre en compte la souveraineté de cet Etat dans la mise en œuvre de mesures de légitime défense. Ainsi, il conviendra de demander le consentement de cet Etat pour prendre des mesures sur son territoire. En cas d'absence de consentement ou d'autorisation d'intervention accordée par le Conseil de sécurité des Nations Unies, une minorité d'experts considère qu'il est impossible d'intervenir alors qu'une majorité d'experts considère : « *The majority concluded that self-defence against a cyber armed attack in these circumstances is permissible when it complies with the principle of necessity (Rule 72), is the only effective means of defence against the armed attack, and the territorial State is unable (e.g., because it lacks the expertise or technology) or unwilling to take effective actions to repress the relevant elements of the cyber armed attack. In particular, these Experts emphasised that States have a duty to ensure their territory is not used for acts contrary to international law (Rule 6).* » (commentaire sous la règle 71 – §25, p. 347). **La majorité des experts reprend ici l'approche américaine**

---

68 *Ibid.*, p. 103, para 195.

« *unwilling unable* », justifiant le recours à la force dans le cadre de la mise en œuvre du droit de légitime défense sur le territoire d'un Etat qui est incapable ou réticent à agir contre les responsables de l'agression armée. Les experts soutenant cette approche considèrent que l'Etat doit d'abord demander à l'Etat du territoire concerné de mettre un terme aux activités en question.

La **règle 72** précise que **l'emploi de la force impliquant des cyber opérations dans le cadre de la mise en œuvre du droit légitime défense par un Etat doit être nécessaire et proportionné**.

Il est intéressant de noter la formulation de la règle, qui ne s'applique donc qu'à l'emploi de la force et non à toutes mesures. En ce sens, le commentaire précise ainsi que la nécessité impose que la mise en œuvre de mesures impliquant un emploi de la force n'est possible que lorsque aucune autre option n'est disponible (commentaire sous la règle 72 – §3, p. 349).

Il convient de souligner, néanmoins, que les critères de proportionnalité et de nécessité s'appliquent aussi dans le cadre des contre-mesures. Ainsi, la règle aurait pu être simplifiée en précisant que les mesures prises par un Etat invoquant son droit de légitime défense doivent être nécessaires et proportionnées.

Le point important du commentaire concernant la règle 72 est qu'il est possible de prendre en légitime défense des mesures numériques ou physiques contre une agression armée qu'elle soit numérique ou non (commentaire sous la règle 72 – §5, p. 349).

La **règle 73** précise que **le droit d'employer la force en légitime défense résulte lorsqu'une agression armée survient ou est imminente. La condition d'immédiateté s'applique aux mesures prises**.

Le commentaire rappelle que l'article 51 de la Charte des Nations Unies permet d'invoquer le droit de légitime défense lorsque l'Etat « *est l'objet d'une agression armée* », c'est-à-dire lorsque l'agression armée a commencé à produire ses effets ou lorsqu'elle a été initiée mais n'a pas encore commencé à produire ses effets (commentaire sous la règle 73 – §1, p. 350).

Le groupe d'experts est de l'avis que même si ce n'est pas expressément prévu par l'article 51, les Etats disposent d'un droit de légitime défense anticipée. Les paragraphes 2 à 10 de la règle 73 discutent de cette question. Le groupe d'experts souligne que « *a State need not wait idly as the enemy prepares to attack. Instead, a State may defend itself once an armed attack is 'imminent'. Such action is labelled 'anticipatory self-defence' in international law.* » (commentaire sous la règle 73 – §2, p. 350).

Afin de simplifier le propos, nous rappelons les différentes formes de légitime défense et de légitime défense anticipée qui peuvent être envisagées :

1. L'action a commencé et produit ses effets ;
2. L'action a commencé, produit ses effets mais ils n'atteignent pas encore le seuil de l'agression armée ;
3. L'action a commencé mais ne produit pas encore ses effets (**légitime défense '*interceptive*'**)[69], il s'agit par exemple du tir d'un missile, l'agression armée commence avec le tir du missile et non au moment où il explose et produit ses effets ;
4. L'action n'a pas commencé mais est imminente (**légitime défense préemptive**) ;

---

69 Cette approche a été notamment développée par Yoram Dinstein qui prend comme exemple hypothétique l'attaque japonaise contre Pearl Harbor en 1941, suggérant que dans ce cas les américains auraient pu invoquer le droit de légitime défense '*interceptive*' à partir du moment où les avions japonais étaient en route vers Hawaii et sans attendre qu'ils atteignent leur cible. DINSTEIN Y., *War, aggression, and self-defence*, 5e éd., New York, Cambridge University Press, 2012, p. 204.

5. La situation pourrait conduire à une agression armée sans qu'aucune action n'ait commencé ou soit en préparation (**légitime défense préventive**), il s'agit par exemple du cas où un Etat invoque le droit de légitime défense contre un Etat développant des armes chimiques ou nucléaires car elles pourraient représenter une menace dans le futur.

Les deux premières formes ne posent pas de problème particulier, l'agression armée est en cours et l'Etat victime peut invoquer son droit de légitime défense. La troisième forme est une nuance de la deuxième. Les experts du *Manuel de Tallinn 2.0* ne considèrent pas cette nuance comme pertinente dans leur analyse car la vitesse de propagation et d'action des cyber opérations la rend, selon eux, inopérante (commentaire sous la règle 73 – §3, p. 351).

Les quatrième et cinquième formes constituent des formes de légitime défense anticipée.

Concernant la légitime défense préemptive, la majorité des experts rejette le critère de la proximité temporelle et lui préfère le critère de la « *dernière fenêtre d'opportunité* » pour agir, c'est-à-dire que l'Etat visé peut agir en légitime défense anticipée lorsque l'Etat auteur est clairement engagé dans la mise en œuvre de son agression armée et que l'Etat visé va perdre sa dernière chance d'agir efficacement contre cette action à venir (commentaire sous la règle 73 – §4, p. 351). Certains experts au sein de cette majorité considèrent qu'en plus du critère de la dernière fenêtre d'opportunité, il est nécessaire de prendre en compte le facteur temporel et donc l'imminence de l'agression armée (§5, p. 352). Dans le cadre de la mise en œuvre de la légitime défense anticipée, il est important de bien distinguer les actions constituant la phase initiale de l'agression armée de celles qui ne sont que préparatoires. Seules les premières peuvent justifier l'invocation de la légitime défense anticipée (§§7-8, p. 352).

Le groupe d'experts rejette unanimement la légitime défense préventive (commentaire sous la règle 73 – §10, p. 353), soulignant que le fait qu'un Etat belliqueux dispose des capacités nécessaires pour lancer des cyber agressions armées n'est pas suffisant pour permettre d'invoquer la légitime défense anticipée contre cet Etat. Il convient ici de souligner que précédemment, dans le commentaire de la règle 71, le groupe d'experts a noté « *A case illustrating the unsettled nature of the armed attack threshold is that of the 2010 Stuxnet operation. In light of the damage the operation caused to Iranian centrifuges, some members of the International Group of Experts were of the view that it reached the armed attack threshold (unless justifiable on the basis of anticipatory self-defence (Rule 73)).* » (commentaire sous la règle 71 – §10, p. 342). Ainsi, le groupe d'experts rejette expressément la légitime défense préventive dans le commentaire de la règle 73, mais semble lui avoir porté un certain crédit dans le commentaire sous la règle 72, peut-être parce qu'il s'agissait là du cas particulier des armes nucléaires.

En conclusion sur les formes de légitime défense anticipée, il convient de souligner que la légitime défense préventive est clairement interdite en droit international. Concernant la légitime défense préemptive, elle n'est pas permise par la Charte des Nations Unies mais la pratique de certains Etats pourrait amener une évolution du droit international coutumier sur ce point.

La condition d'immédiateté (commentaire sous la règle 73 – §§12-13, p. 353-354), spécifiée dans la deuxième partie de la règle, impose que les mesures prises en légitime défense le soient dans un délai raisonnable après la fin de l'agression armée pour ne pas être considérée comme des formes illicites de représailles.

La **règle 74** précise que **le droit de légitime défense peut être mis en œuvre collectivement**, reprenant ici l'article 51 de la Charte des Nations Unies. Elle précise, en outre, que **la légitime défense collective contre une cyber agression armée n'est possible qu'à la demande de l'Etat victime et dans les limites établies par cette demande**.

La **règle 75** reprend aussi une partie de l'article 51 de la Charte des Nations Unies et précise que **les mesures impliquant des cyber opérations mises en œuvre par un Etat dans l'exercice**

de son droit de légitime défense sur la base l'article 51 de la Charte des Nations Unies doivent être immédiatement portées à la connaissance du Conseil de sécurité.

4.1.2 Sécurité collective (chapitre 15 – règles 76 à 79)

Le quinzième chapitre du *Manuel de Tallinn 2.0* s'intéresse à la sécurité collective et comprend quatre règles (règles 76 à 79) : la règle 76 était présente dans la première édition (règle 18) mais a subi une modification mineure, la règle 77 est inchangée par rapport à la première édition (règle 19), alors que les règles 78 et 79 sont nouvelles.

La **règle 76** précise que **si le Conseil de sécurité constate qu'une cyber opération constitue une menace contre la paix, une rupture de la paix ou un acte d'agression, il peut autoriser des mesures n'impliquant pas l'emploi de la force armée, notamment des cyber opérations, en réponse. Si le Conseil de sécurité estime que ces mesures sont inadéquates, il peut décider la mise en œuvre de mesures impliquant l'emploi de la force armée, notamment des cyber opérations**.

La règle était présente dans la première édition du Manuel de Tallinn (règle 18), et a été modifiée dans la nouvelle édition pour y ajouter « , en réponse » à la fin de la première phrase. Il s'agit d'une modification mineure n'affectant en rien le sens de la règle. Cette règle reprend les articles 39 à 42 de la Charte des Nations Unies.

Le commentaire rappelle à juste titre que jusqu'à présent, le Conseil de sécurité n'a jamais constaté qu'une cyber opération constituait une menace contre la paix, une rupture de la paix ou un acte d'agression (commentaire sous la règle 76 – §1, p. 357).

La **règle 77**, reprise de la première édition sans modification, précise que **les organisations, accords ou agences à caractère régional peuvent mener des actions coercitives, impliquant des cyber opérations ou en réponse à des cyber opérations, en vertu d'un mandat ou d'une autorisation du Conseil de sécurité des Nations Unies**. Cette règle reprend les chapitres VII et VIII de la Charte des Nations Unies.

La **règle 78** précise que **durant la conduite d'opérations de paix, les Etats peuvent mettre en œuvre des cyber opérations en conformité avec le mandat de l'opération de paix et du droit international applicable**.

La **règle 79** comporte deux alinéas. Le premier alinéa précise que **tant qu'ils bénéficient de la protection accordée aux civils et aux objets civils par le droit des conflits armés, les personnels, installations, matériels, unités et véhicules des Nations Unies, notamment les ordinateurs et les réseaux informatiques utilisés dans le cadre des opérations des Nations Unies, doivent être respectés et protégés et ne doivent pas être visés par des cyber attaques**. Le second alinéa précise que **les autres personnels, installations, matériels, unités ou véhicules, notamment les ordinateurs et réseaux informatiques, utilisés dans le cadre de missions d'assistance humanitaire ou de maintien de la paix en vertu de la Charte des Nations Unies sont protégés contre les cyber opérations aux termes des mêmes conditions**.

4.2 Droit des cyber conflits armés (Part IV. The law of cyber armed conflict – pp. 373 à 562 – règles 80 à 154)

La dernière partie du *Manuel de Tallinn 2.0* s'intéresse à l'applicabilité et l'application du droit des conflits armés aux cyber opérations. Elle comporte cinq chapitres traitant respectivement :

- Chapitre 16 – le droit des conflits armés en général (règles 80 à 85) ;
- Chapitre 17 – la conduite des hostilités (règles 86 à 130) ;
- Chapitre 18 – certaines personnes, objets et activités (règles 131 à 145) ;
- Chapitre 19 – occupation (règles 146 à 149) ;
- Chapitre 20 – Neutralité (règles 150 à 154).

Il convient de souligner que cette partie était déjà présente dans la première édition du *Manuel de Tallinn* et que la majorité des règles sont inchangées ou ont subi des modifications mineures.

5 Conclusion

Le *Manuel de Tallinn 2.0* est un travail d'une grande qualité réalisé par un groupe d'experts renommés. Cet ouvrage a le mérite d'offrir un panorama relativement complet des règles de droit international applicables aux cyber opérations.

Cette analyse a une double vocation. Premièrement, offrir un résumé des règles du Manuel de Tallinn 2.0 en français, permettant ainsi aux lecteurs francophones de disposer d'un document relativement court retraçant le contenu des règles du *Manuel de Tallinn 2.0*. Deuxièmement, offrir une analyse des points clefs du *Manuel de Tallinn 2.0* et notamment des points les plus sensibles et ceux où l'approche du *Manuel* pourrait être considérée comme discutable.

En ce sens, il nous parait utile de lister en conclusion les principales remarques et critiques qui ont été formulées dans cette analyse au regard du contenu du *Manuel de Tallinn 2.0* :

- L'absence de règle générale sur la licéité des cyber opérations (voir titre 3.2, p. 15)[70] ;
- L'existence, selon les experts du *Manuel de Tallinn*, d'un seuil d'intensité pour qualifier la violation de la souveraineté (voir titre 3.2.1.2.1, pp. 18-19) ;
- La question de la souveraineté des États sur leurs données sensibles et stratégiques (voir pp. 16-17 et 20) ;
- L'existence d'un seuil d'intensité pour l'obligation de diligence (voir pp. 22-23) ;
- Les experts du *Manuel* considèrent qu'il n'y a pas d'obligation d'offrir de négocier avant de prendre des contre-mesures (voir p. 32) ;
- Le soutien implicite à la théorie des contre-mesures armées, même si officiellement le *Manuel* la rejette (voir pp. 33-34) ;
- La question des contre-mesures collectives et de l'assistance (voir p. 35) ;
- L'état de nécessité comme justification pour un recours à la force (voir p. 37) ;
- La conduite de cyber opérations par des organisations internationales (voir p. 39-40) ;
- L'approche ambiguë du manuel sur l'espionnage, qui reprend l'approche traditionnelle dans la règle 32 mais dont le commentaire semble apporter un certain crédit à l'approche selon laquelle tout acte d'espionnage serait licite (voir principalement pp. 43-45) ;
- Le traitement accordé aux droits de l'homme, qui est très général et imprécis, et qui laisse une très grande marge d'appréciation aux Etats (voir pp. 47-48)[71] ;
- L'approche sur l'applicabilité du principe de non-intervention aux organisations internationales (voir pp. 56-57) ;
- Le traitement des seuils de l'emploi de la force et de l'agression armée (voir p. 61).

Il convient de rappeler que ces remarques et critiques n'engagent que l'auteur de cette analyse et qu'elles ne viennent en rien remettre en cause la qualité et le sérieux du travail du groupe d'experts à l'origine du *Manuel de Tallinn 2.0*. Il s'agit surtout d'indiquer au lecteur des points précis où l'approche adoptée aurait pu être différente ou prendre en compte de manière plus explicite la diversité des approches et des désaccords.

---

70 Les renvois font références aux titres de la présente analyse et non du *Manuel de Tallinn 2.0*.

71 Je reprends ici les critiques formulées dans : INGBER R., « Interpretation Catalysts in Cyberspace », *op. cit.* ; POKEMPNER D., « Squinting through the Pinhole: A Dim View of Human Rights from *Tallinn 2.0* [*Symposium:* Tallinn Manual 2.0 *on the International Law Applicable to Cyber Operations*] », *op. cit.*

6 Bibliographie sélective

Cette bibliographie identifie des articles et commentaires concernant les règles et commentaires contenus dans le *Manuel de Tallinn 2.0*. Il ne s'agit pas d'une bibliographie sur les normes de droit international applicables aux cyber opérations.

BANKS W.C., « State Responsibility and Attribution of Cyber Intrusions after *Tallinn 2.0* [*Symposium:* Tallinn Manual 2.0 *on the International Law Applicable to Cyber Operations*] », *Texas Law Review*, 2017 2016, vol. 95, p. 1487-1513.

CORN G.P., *Tallinn Manual 2.0 – Advancing the Conversation*, https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/.

CORN G.P. et R. TAYLOR, « Sovereignty in the Age of Cyber », *AJIL Unbound*, 2017, vol. 111, p. 207-212, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/sovereignty-in-the-age-of-cyber/02314DFCFE00BC901C95FA6036F8CC70.

GHAPPOUR A., « Tallinn, Hacking, and Customary International Law », *AJIL Unbound*, 2017, vol. 111, p. 224-228, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/tallinn-hacking-and-customary-international-law/9A66B622C2AC43319D8FA45C75D8B5D2.

GINSBURG T., « Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0 », *AJIL Unbound*, 2017, vol. 111, p. 205-206, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/introduction-to-symposium-on-sovereignty-cyberspace-and-tallinn-manual-20/F54618BA6651E6E706A45365B6647FC8.

INGBER R., « Interpretation Catalysts in Cyberspace [*Symposium:* Tallinn Manual 2.0 *on the International Law Applicable to Cyber Operations*] », *Texas Law Review*, 2017 2016, vol. 95, p. 1531-1554.

JENSEN E.T., « The Tallinn Manual 2.0: Highlights and Insights », *BYU Law Research Paper No. 17-10*, 2017, https://ssrn.com/abstract=2932110.

JENSEN E.T. et S. WATTS, « A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer [*Symposium:* Tallinn Manual 2.0 *on the International Law Applicable to Cyber Operations*] », *Texas Law Review*, 2017 2016, vol. 95, p. 1555-1578.

LIU I.Y., « The due diligence doctrine under Tallinn Manual 2.0 », *Computer Law & Security Review: The International Journal of Technology Law and Practice*, juin 2017, vol. 33, n° 3, p. 390-395, http://www.sciencedirect.com/science/article/pii/S0267364917301127.

MAČÁK K., *From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers*, Rochester, NY, Social Science Research Network, 2017, https://papers.ssrn.com/abstract=2961821.

OHLIN J.D., « Did Russian Cyber Interference in the 2016 Election Violate International Law [*Symposium:* Tallinn Manual 2.0 *on the International Law Applicable to Cyber Operations*] », *Texas Law Review*, 2017 2016, vol. 95, p. 1579-1598.

POKEMPNER D., « Squinting through the Pinhole: A Dim View of Human Rights from *Tallinn 2.0* [*Symposium:* Tallinn Manual 2.0 *on the International Law Applicable to Cyber Operations*] », *Texas Law Review*, 2017 2016, vol. 95, p. 1599-1618.

REEVES S.R. et R.E. BARNSBY, « Give Them an Inch, They'll Take a Terabyte: How States May Interpret *Tallinn Manual 2.0*'s International Human Rights Law Chapter [*Symposium:* Tallinn

Manual 2.0 *on the International Law Applicable to Cyber Operations*] », *Texas Law Review*, 2017 2016, vol. 95, p. 1515-1530.

SCHALLER C., « Beyond Self-Defense and Countermeasures: A Critical Assessment of the *Tallinn Manual*'s Conception of Necessity [*Symposium:* Tallinn Manual 2.0 *on the International Law Applicable to Cyber Operations*] », *Texas Law Review*, 2017 2016, vol. 95, p. 1619-1638.

SCHMITT M.N., « Grey Zones in the International Law of Cyberspace », *The Yale Journal of International Law Online*, 2017, vol. 42, n° 2, p. 1-21, https://campuspress.yale.edu/yjil/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf.

SCHMITT M.N. et L. VIHUL, « Sovereignty in Cyberspace: *Lex Lata Vel Non*? », *AJIL Unbound*, 2017, vol. 111, p. 213-218, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/sovereignty-in-cyberspace-lex-lata-vel-non/6C6FD06E2B02B72224DF7127483A33F0.

SPECTOR P., « In Defense of Sovereignty, in the Wake of Tallinn 2.0 », *AJIL Unbound*, 2017, vol. 111, p. 219-223, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/in-defense-of-sovereignty-in-the-wake-of-tallinn-20/8B742A410CCBED0E4967BB7FB15D3D7D.

VIHUL L. et M.N. SCHMITT, « Respect for Sovereignty in Cyberspace Symposium: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations », *Texas Law Review*, 2017 2016, vol. 95, p. 1639-1670.

WOODS A.K., *The Tallinn Manual 2.0, Sovereignty 1.0*, https://www.lawfareblog.com/tallinn-manual-20-sovereignty-10.